Fallback Algorithms for Line Current Differential Protection Applied With Asymmetrical Channels Upon the Loss of Time Reference

B. Kasztenny, N. Fischer, and B. Le
Schweitzer Engineering Laboratories, Inc.

Presented at the
11th International Conference on Developments in Power System Protection
Birmingham, United Kingdom
April 23–26, 2012

FALLBACK ALGORITHMS FOR LINE CURRENT DIFFERENTIAL PROTECTION APPLIED WITH ASYMMETRICAL CHANNELS UPON THE LOSS OF TIME REFERENCE

B. Kasztenny*, N. Fischer*, B. Le*

*Schweitzer Engineering Laboratories, Inc., 2350 NE Hopkins Court, Pullman, WA 99163 USA,
Bogdan_Kasztenny@selinc.com

Keywords: Line current differential protection, asymmetrical channels, absolute time reference, data alignment, time fallback.

Abstract

When applied over asymmetrical or potentially asymmetrical channels (unequal channel propagation times in the transmitting and receiving directions), such as commercial-class SDH/SONET networks, line current differential schemes need an external time reference for current data alignment if the sensitivity of the differential scheme is to be preserved. Modern line differential schemes can handle a limited amount of asymmetry (2 to 3 milliseconds) without the need for an external time source, but they sacrifice sensitivity in the process. Such reliance on external time sources increases both the cost and complexity of line current differential scheme applications. The usage of external time, however, may be unavailable in some situations.

Line current differential 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 beyond the point of safe usage in protection applications. This is often referred to as time fallback logic. This paper presents several time fallback modes, varying with respect to balancing protection security and dependability.

1 Introduction

Responding to all currents bounding the zone of protection, the current differential principle has a very high potential for both sensitivity (effectively, it sees the fault current at the place of an internal fault) and security (effectively, it sees an external fault current flowing in and out of the protection zone). Also, differential protection is typically easy to apply because it does not require detailed short-circuit studies and settings calculations.

In its application to power lines, the differential principle is immune to weak terminals, series compensation, changing short-circuit levels, current inversion, power swings, nonstandard short-circuit current sources such as power electronics-based distributed generation, and many other issues relevant for protection techniques based on measurements from a single line terminal [1].

Microprocessor-based relays using the differential principle need current data to have the same time reference. In bus, transformer, or generator protection, this is accomplished naturally by using a single protective device that directly receives all the required currents and samples them in a synchronized fashion. Microprocessor-based line current differential (87L) schemes need an explicit method to synchronize or align the currents taken by separate 87L relays at various line terminals.

One aspect of data alignment is concerned with time-stamping the current data. Two methods are used practically in this respect.

When using symmetrical channels, 87L schemes typically align the data using the industry standard method known as the ping-pong algorithm (see Section 2). When the channel is not symmetrical, the ping-pong algorithm introduces a time alignment error proportional to the amount of asymmetry, which yields a current phase error, which, in turn, creates a fictitious differential signal.

Therefore, when using asymmetrical channels, the 87L relays require a common (external) time reference to drive the current sampling (see Section 3). Historically, Global Positioning System (GPS) clocks that are either embedded in the 87L relays (rarely) or are standalone and connected via an IRIG-B input (more commonly) have been used as the time reference.

Reliance on external time sources makes the scheme more complex because care must be taken to correctly engineer the timing network and less available due to the sheer number of its components. In one important aspect, the scheme must be programmed to deal with the situations when the required time sources are unavailable or report degraded quality of provided time information.

After reviewing the channel-based (ping-pong) and external time-based alignment methods in Sections 2 and 3, this paper explains potential issues with the time sources (Section 4) and focuses on fallback strategies for the loss of the time sources (Section 5). Criteria impacting a fallback mode are discussed in Section 6, while Section 7 provides several application examples.

2 Channel-based data alignment

In this paper, we follow the concept of a clock offset. Assume two 87L relays that communicate over a channel use independent free-running clocks to time-stamp their current data. In order to align the local and remote data and use the data in differential calculations, the relays need to know the clock difference (offset) between the two free-running clocks. As the clocks drift very slowly, the clock offset changes very slowly, simplifying the process of estimating it.

In this section, we briefly review the channel-based clock offset calculation method (ping-pong) [4].

Refer to Fig. 1. 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.

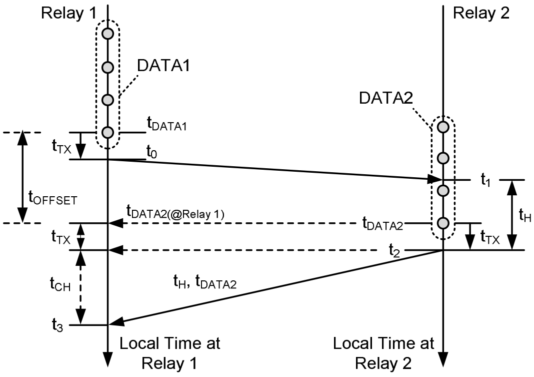

Fig. 1. Illustration of the channel-based alignment method.

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 after the channel delay time. 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:

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

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

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

The data time stamp expressed in Relay 2 time is included in the packet. This allows calculation of the time offset:

$$\begin{aligned} t_{OFFSET} &= t_{DATA2(@\text{Relay}1)} - t_{DATA2} \\ &= t_3 - t_{CH} - t_{TX} - t_{DATA2} \end{aligned} \tag{4}$$

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:

$$t_{DATA2(@\text{Relay}1)} = t_{DATA2} + t_{OFFSET} \tag{6}$$

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, the method 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 synchronous optical network/synchronous digital hierarchy (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 elements. In such a case, the calculated clock offset is 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.

3 Time-based data alignment

Data alignment using the channel-based method is often considered superior because it does not require the usage of explicit time sources to be a part of the line protection scheme.

Any given 87L operating characteristic handles alignment errors to a certain degree [5]. However, if the channel asymmetry is beyond the permissible limits given the targeted sensitivity and settings of the 87L function (typically 2 to 4 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 were GPS-synchronized. Now there are terrestrial, network-based time-distribution schemes [2].

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, 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:

$$t_{OFFSET} \equiv 0 \tag{7}$$

The remainder of the data alignment algorithm, starting with (6), works identically as in the channel-based mode.

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 [4]. 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.

4 Concerns with time sources

4.1 Satellite clocks

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. Solar flares, GPS jamming, and GPS spoofing, although interesting, are fortunately very rare [2].

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.

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. 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.

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.

4.2 Availability of time-distribution circuits

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 rigorous commissioning procedures and periodic testing programs.
- 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.

5 Time fallback algorithms

5.1 Principles

Table 1 explains several time fallback modes, progressing from the simplest (and most secure) to more elaborate solutions that attempt to enhance dependability of the 87L scheme.

5.2 Channel monitoring fundamentals

As explained in Table 1, some channel characteristics need to be measured in order to feed into the time fallback logic.

The roundtrip 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. 1):

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

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. 1 and consider 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:

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

Mode	Details 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 [4]. 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 (asymmetry below a factory constant), 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 (asymmetry below a factory constant), 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 roundtrip channel delay (step change greater than a factory constant) 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 1: Summary of typical time fallback modes.

5.3 Implementation

Modes 1 and 2 are straightforward. Fig. 2 better illustrates Modes 3 and 4. The figure applies to Mode 4. Note, however, that Mode 3 is a subset of Mode 4.

In reference to Fig. 2, when the fallback mode is requested, the relay checks if the channel was symmetrical at the moment of losing time reference [measured using (9) and (10)]. If the channel was symmetrical and working properly prior to the need for fallback, the relay engages channel-based alignment [i.e., uses (5) to calculate the clock offset]. When in channel-based alignment, the relay stays there as long as fallback is required, unless the channel exhibits a step change in the roundtrip time [measured using (8)]. The step change signifies channel switching and potential asymmetry. Note that after the time reference is lost, (9) and (10) cannot be executed anymore.

When the channel is switched or was not symmetrical at the moment of requesting the time fallback, the scheme applies fallback Mode 2.

When the request for fallback is removed (time sources are back in service and in tolerance), the relay switches back to the time-based alignment [i.e., uses (7) to calculate the clock offset].

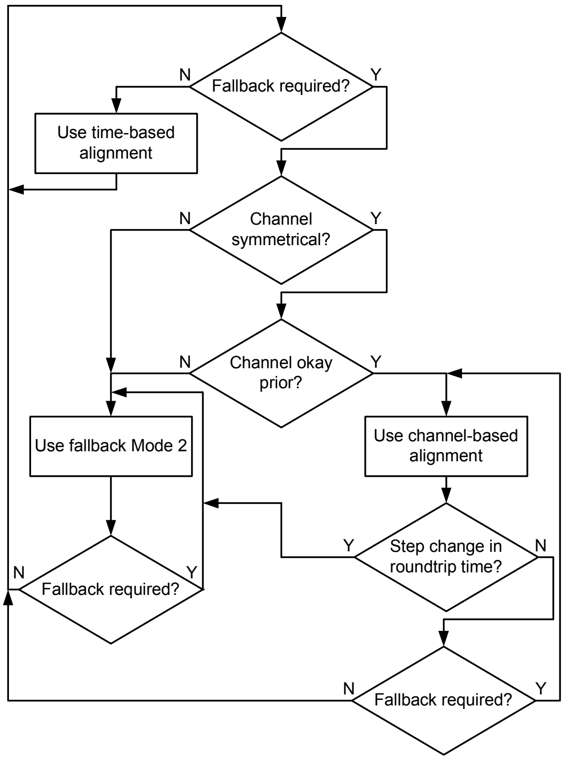

Fig. 2. Flow chart of time fallback Mode 4.

6 Selection considerations

6.1 Applicability for a given 87L installation

Table 2 reviews the suitability of the four time fallback modes to typical line current differential applications, including two- and three-terminal lines, single or redundant channels, and master or slave operation [5].

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.

Table 2: Merits of the introduced time fallback modes.

6.2 Regulatory requirements and applied protection philosophy

In the case of high-voltage line protection, it is common utility practice to apply two individual, separate, and parallel redundant protection systems for any given transmission line, particularly those where a delayed clearance or failure to trip for a fault can lead to consequent cascading outages or a loss of wide-area system stability in the bulk electric system (BES). Additionally, should such circuits be forced out of service manually due to a loss of protection, this can cause violations of other criteria (e.g., stability, loadability, and thermal limits), which can cause a utility or regional system coordinator to be forced to take additional actions to reduce load and potentially arm or enable additional system integrity protection schemes (SIPSs). Such circuits have significant operational impact on the BES and are commonly referred to as BES-impactive circuits.

Such BES-impactive circuits must usually cater to single contingency events that can remove part or all of a protection system from service (including failures as well as routine maintenance of protection system elements), hence the requirement for redundant protection schemes. In this way, a single contingency such as loss of potential, loss of a channel, or loss of a time source used by an 87L scheme will not cause both protection systems to become unavailable. Therefore, there is no danger of a delayed trip or a failure to trip.

Protection system designs that follow full redundancy will typically apply time fallback Mode 1 when using 87L schemes with external time sources. With the second system being fully operational, there is no need to extend dependability of the 87L scheme at the expense of security.

Nonredundant protection systems, or a redundant system that lost one of the parallel protection schemes due to maintenance or failure, may opt for time fallback Modes 2, 3, or 4 depending on the details of application and user preferences. This gives a chance to continue to protect the line and avoids a forced line outage.

Should time fallback fail and the 87L element become unavailable, backup functions often integrated in the 87L relays are typically engaged. These include stepped distance backup, underreaching instantaneous Zone 1, Zone 1 extension logic, overcurrent, or directional comparison schemes [3].

7 Application examples

Fig. 3, Fig. 4, and Fig. 5 illustrate some of the typical scenarios for the introduced time fallback modes.

Consider the two-terminal, dual-channel application depicted in Fig. 3. 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. 3 to lose dependability.

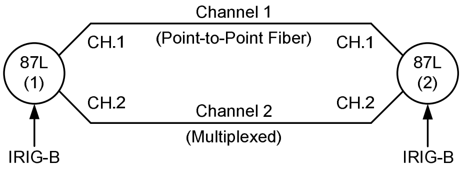

Fig. 3. Two-terminal application with redundant channels.

Consider the three-terminal master application depicted in Fig. 4. 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.

Consider the two-terminal, single-channel application depicted in Fig. 5. 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.

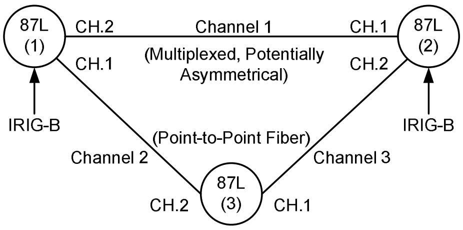

Fig. 4. Three-terminal application with three channels.

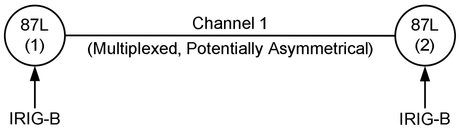

Fig. 5. Two-terminal application with a single, potentially asymmetrical channel.

If the channel asymmetry was small at the moment of losing time, the relays will switch to the channel-based mode, engaging high-security mode and continuing to provide protection. If the channel is subsequently switched in the multiplexed network, as detected by step change in the roundtrip 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.

8 Conclusion

Line current differential protection provides sensitive and inherently selective protection. It brings the benefit of easy settings selection and is immune to many system conditions. However, the principle is communications-based with several consequences. The need to use external time sources for data alignment when utilizing asymmetrical channels is one of them. It is typically recommended to avoid using time sources in protection applications if a symmetrical communications channel can be provisioned.

If asymmetrical channels are used for 87L protection, reliance on external time sources is a must. These sources must be engineered and maintained to protection standards. In addition, the scheme must include time fallback in order to respond to the loss of time in a manner satisfying the given protection philosophy of the user. Selection of a time fallback mode needs to consider protection redundancy and regulatory requirements as well as the internal relay philosophies of the user.

References

[1] H. J. Altuve Ferrer and E. O. Schweitzer, III (eds.), *Modern Solutions for Protection, Control, and Monitoring of Electric Power Systems.* Schweitzer Engineering Laboratories, Inc., Pullman, WA, 2010.

[2] 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.

[3] S. Hodder, B. Kasztenny, and N. Fischer, “Backup Considerations for Line Current Differential Protection,” proceedings of the 65th Annual Conference for Protective Relay Engineers, College Station, TX, April 2012.

[4] B. Kasztenny, N. Fischer, K. Fodero, and A. Zvarych, “Communications and Data Synchronization for Line Current Differential Schemes,” proceedings of the 38th Annual Western Protective Relay Conference, Spokane, WA, October 2011.

[5] 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.

Previously presented at the 11th International Conference
on Developments in Power System Protection.