Backup Considerations for Line Current Differential Protection

Steven Hodder, *Hydro One Networks, Inc.*
Bogdan Kasztenny and Normann Fischer, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Line current differential (87L) protection relies on communications for the exchange of current values and, if applied over asymmetrical channels, on external time sources for current alignment. Proper engineering of 87L schemes calls for a backup strategy that considers the loss of communications and/or the loss of external time sources.**

This paper reviews various channel and time backup strategies for 87L protection schemes and considers utility practices and regulatory constraints related to line protection redundancy, forced line outages, preferred balance between protection dependability and security, ability to provide adequate protection coverage with distance or overcurrent elements, and availability of an independent pilot channel for directional comparison backup schemes.

I. INTRODUCTION

Line current differential (87L) is a protection principle that provides sensitive and inherently selective protection of overhead lines and cables, in addition to the benefits of easy settings selection and immunity to changing and unusual system conditions. The latter includes weak infeed conditions, series compensation, power swings, and nonstandard short-circuit current sources, such as inverter-based distributed generation [1].

While providing all these benefits, 87L schemes are dependent on communications, with several crucial consequences.

First, proper application of 87L schemes requires knowledge of long-haul communications in the electric power system, such as direct fiber links or multiplexed channels [2] [3].

Second, testing 87L schemes is more involved when compared with other line protection schemes because multiple relays located at different line terminals must communicate in order to calculate the differential signal [4].

Last, but not least, reliance on communication impacts the availability of 87L schemes. In one aspect, a failure of a nonredundant channel makes the scheme unavailable. In another aspect, channel asymmetry may require using external time sources for data alignment [2] [5] [6]. In such cases, reliance on external time sources further impacts 87L availability.

This paper addresses the availability of 87L schemes and considers various backup strategies for the loss of 87L element functionality.

Parallel redundancy is assumed as a means to address issues with current transformers (CTs), wiring, relays, breaker trip coils, battery systems, and communications channels in general. We therefore focus on the availability of 87L elements only in the context of problems with communications and time sources (if used).

In Section II, we review and explain conditions that can render 87L elements unavailable. This includes discussions on redundant 87L channels, the master-slave operating mode, problems aligning 87L currents, intentional blocking of 87L elements, relay out-of-service conditions, and so on.

In Section III, we discuss regulatory constraints and internal utility rules related to forced line outages upon the loss of protection, loss of instantaneous/high-speed fault clearing ability, or reduction of protection sensitivity. These rules impact both the original protection scheme design and the backup strategy for the 87L elements. This section starts with a general discussion and progresses to include North American Electric Reliability Corporation (NERC) requirements and specific practices of a major North American utility.

In Section IV, we consider channel redundancy and 87L backup in general.

In Section V, we review protection elements typically applied to back up 87L schemes for the loss of channel or loss of time reference. This includes single-ended methods (stepped distance, including Zone 1 extension and overcurrent) and directional comparison (DC) schemes.

In Section VI, we discuss different ways of implementing 87L backup schemes. These range from parallel redundancy (the 87L element and its backup fully operational and working in parallel) to adaptive schemes that engage or modify the backup function in response to the status of the 87L element at any given time.

Channel routing is an important consideration for the availability and independence of 87L communications. Channel diversity is typically considered with respect to the right of way of the protected line, the redundant 87L channel (if used), and the channel for a DC backup scheme. Therefore, in Section VII, we discuss communications path selection for maintaining availability of protection and avoiding common-mode failures in the communications system.

Section VIII concludes the paper, gathering some key observations and recommendations.

II. CONDITIONS MAKING LINE DIFFERENTIAL PROTECTION UNAVAILABLE

Several channel and time reference conditions can render 87L elements unavailable. Some applications provide for considerable ride-through and fallback abilities upon channel issues. It is therefore beneficial to understand the response of a particular 87L relay design to channel impairments before selecting the backup scheme.

A. Loss of Communications

Any 87L scheme needs access to all currents surrounding the differential zone. The loss of a channel that is required at a particular time by the 87L element (given the details of the application) for deriving the differential signal can prevent the element from operating as expected.

The following several scenarios can apply within the general category of loss of communications.

1) Two-Terminal Applications With Redundant Channels

Fig. 1a shows two channels used concurrently to provide independent communications between two 87L relays. The relays incorporate hot standby logic to switch to the standby channel upon a major problem with or complete loss of the primary channel. This way, the loss of one channel does not lead to the unavailability of the 87L scheme, assuming the other channel is operational. Depending on the characteristics of the standby channel, the scheme performance may be affected. The operating time (due to different latency of the standby channel) or the availability (due to the different bit error rate [BER] of the standby channel) may change.

2) Three-Terminal Applications With Three Channels

Fig. 1b shows an 87L scheme that can switch to the master-slave mode, whereby the two relays that lose the mutual channel (Relays 1 and 2) serve the current data to the master (Relay 3). The master relay receives all required currents, provides the 87L function, and, upon a line fault, orders the slave relays to trip the remote breakers directly using in-band direct transfer trip (DTT) bits. This way, a loss of one channel does not lead directly to the unavailability of the overall 87L protection. The slave relays would trip for internal faults after a short extra time delay required for the direct trip command to travel back from the master relay.

3) Combination of Stub Bus and Master-Slave Operation

Multiterminal or tapped lines can be left in service with one terminal isolated via a line disconnect switch while the local breaker or breakers are closed, such as to maintain the integrity of a ring bus or to keep the two buses tied in the breaker-and-a-half configuration. This is referred to as stub bus mode. In the stub bus, the local relay sends zero value currents and substitutes the received currents with zeros. When it operates, it trips local breaker(s) only (see Fig. 1c). Consider a three-terminal application with one master and two slave relays, while the master is in the stub bus mode depicted in Fig. 1d. Being in the stub bus mode, the master protects the local stub bus and does not send DTT commands to the slave relays for a fault on the protected stub bus. As a result, the line between the two remote terminals and the open disconnect switch is not protected by the 87L element. The 87L element in the master relay is operational but protects the stub bus only; the slave relays are unable to run the differential calculations for the remaining line currents.

Backup protection schemes for three-terminal applications must therefore take into account the local stub bus condition, in addition to the status of the main 87L element.

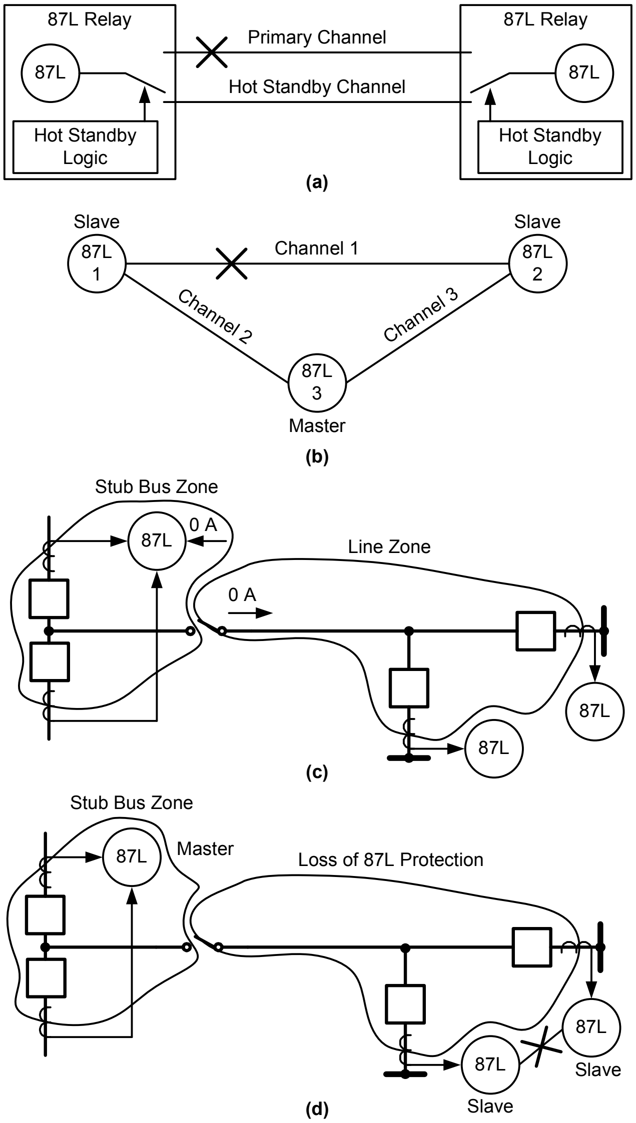

Fig. 1. Selected 87L scheme configurations and relevant operating conditions: two-terminal application with a hot standby channel (a), three-terminal master-slave application (b), stub bus configuration (c), and a combination of stub bus and master-slave operation (d).

4) Channel Brownout Conditions

Channel brownout refers to a condition when a channel operates intermittently with a very high percentage of corrupted bits (lost 87L packets), such as during periods of elevated and persistent noise typically caused by a failing component or malfunction of the communications equipment (more prevalent in microwave and leased digital circuits). In such conditions, the channel availability (i.e., the percentage of time the channel is actually operational) is low, leading to a proportionally low, if not worse, availability of the 87L elements. If the channel availability falls below required levels, even though the channel operates intermittently, a user could consider taking the 87L elements out of service (manually or automatically via user-programmable channel alarms) and engaging the 87L backup accordingly.

B. *Problems Aligning Local and Remote Currents*

In order to use the remote currents, each 87L relay must be able to align them with the local currents.

When using symmetrical channels (near equal latency in the transmitting and receiving directions), 87L relays use channel-based alignment based on the industry-accepted ping-pong algorithm [2]. Applications with highly asymmetrical channels (beyond the tolerance of a given relay operating characteristic) require the relays to use external time sources for alignment (historically, satellite clocks connected via high-precision IRIG-B relay inputs) [2].

The 87L element can lose the ability to align the received current data in the following ways:

- In applications configured for channel-based alignment, the following can take place:
  - Counting on symmetrical channels, the 87L relays in this configuration can monitor channel symmetry and suspend 87L operation upon detecting unacceptable levels of asymmetry. This can be done via relay design or via a user-definable channel alarm configured to block the 87L element for security.
  - The 87L relays can fail to reach a proper alignment state if the channel experiences abnormal variability in latency or constantly switches paths (typically due to a malfunction or standing noise in the communications equipment).
- In applications configured for time-based alignment, the following can take place:
  - The 87L relays can lose the IRIG-B connection or be exposed to permanent noise or marginal signal levels in the IRIG-B signal, which prevents the relays from synchronizing to the connected time source.
  - Time sources used in applications configured for external time-based alignment can lose the time reference because of satellite antenna problems, bad weather, or other issues with the Global Positioning System (GPS) [7]. Normally, 87L relays working with external time sources require the sources to comply with the IEEE C37.118 IRIG-B format, which allows the time source to indicate degraded quality of the time information to the connected 87L relay.
  - Applications configured for external time-based alignment typically incorporate several time fallback modes in order to respond to the loss or reduced accuracy of the external timing signals [2]. These fallback modes, however, do not guarantee extending availability upon the loss of the required time source; rather, they give a chance to extend availability under favorable conditions [2]. The worst-case assumption is that the 87L elements that require external time will become unavailable upon the loss of one or more (local or remote) time sources.

C. *87L Element Out-of-Service Condition*

The 87L element can be taken explicitly out of service either by the default relay logic or based on user configuration while the remaining functionality within the multifunction line current differential relay is still operational, including the following examples:

- The built-in channel diagnostics can be configured to block the 87L element upon detecting excessive channel problems in order to remove the danger of misoperation.
- Certain test modes for the 87L elements [4] can disable remote 87L elements when testing the local 87L relay (typically in multiterminal applications or on tapped lines with the local breaker open and the line left energized).
- External loss-of-potential (LOP) conditions in situations where distance elements supervise differential tripping or line charging current is employed [6] can result in either the 87L element falling back into more secure settings or being entirely disabled (based on user preferences).
- User-asserted conditions can block the 87L element while the user performs settings review or other temporary activities.

D. *87L Relay Out-of-Service Condition*

The 87L element can be taken out of service because the entire multifunction 87L relay is taken out of service (power up, settings change process, critical hardware problem, and so on). In this case, the backup protection elements at the remote terminals remaining in service are the only functional protection elements for the given line.

E. *Importance of Monitoring Differential Elements*

From the preceding discussion, it is clear that the availability of 87L elements can change in response to a number of different conditions, including the type of application (standby channels in use or not in use and three-terminal applications), channel status (available or not available and symmetrical or not symmetrical), external time source status (available, degraded, or not available), LOP condition (if voltage-based charging current compensation or distance supervision is used), master-slave mode, stub bus mode, overall relay health (software and hardware alarms), and user-programmable conditions.

As a result, it is beneficial to monitor all these conditions and use 87L status logic that signals the operating condition of the 87L elements. Many 87L relays provide logic for creating and distributing the required status information between the individual relays in the scheme. Some backup strategies might respond and adapt to the current 87L status.

III. Utility Practices and Regulatory Requirements Regarding Protection Availability and Forced Line Outages

In general, the performance of a given protection system is directly tied to the stability and security of the protected power system. In the case of a high-voltage (HV) or extra-high-voltage (EHV) bulk electric system (BES), the critical performance criterion for protection is usually the maximum allowable clearing time for preserving power system stability. Reliability and overall availability of the protection systems associated with a given HV or EHV line are also critically important and must be considered.

A. Line Protection Redundancy

In the case of HV or EHV line protection, it is common utility practice to apply two individual, separate, and parallel redundant protection systems for any given transmission line. This applies, in particular, to lines where a delayed clearance or failure to trip for a fault may lead to consequent cascading outages or a loss of wide-area system stability. Additionally, removing a line from service manually due to a loss of protection may cause violations of other criteria (e.g., stability, loadability, and thermal limits), which may force a utility or regional reliability system coordinator to take additional actions to reduce load and potentially arm additional system integrity protection schemes (SIPSs). Such circuits have significant operational impact on the BES and are commonly referred to as BES-impactive circuits.

In such cases, the maximum allowable fault clearing time for these circuits (including breaker failure time) is very critical to the stability of the BES; therefore, it is essential that the overall protection scheme for the given line operates in a timely manner in order to prevent cascading outages or a loss of wide-area system stability. Such BES-impactive circuits usually must cater for single contingency events that may remove part or all of a protection system from service (including failures and routine maintenance of protection system elements), hence the requirement for redundant protection schemes.

In this case, redundancy specifically refers to functional redundancy where two systems, when presented with the same fault conditions (or other stimulus), behave in an identical manner with the same time sequence and performance. These redundant schemes usually use OR logic such that a decision from either of the two systems is sufficient to make whatever consequent actions occur (as opposed to more complex k-out-of-n voting schemes) [1]. Such redundant schemes are ideally (but not always) provisioned with individual measuring equipment (current and voltage transformers), relay equipment (often, but not necessarily, from different manufacturers), and separate communications hardware and paths (ideally, but not always). This way, a single contingency does not cause both protection systems to become unavailable, preventing either a delayed trip or a failure to trip for a fault or a forced line outage [8].

B. NERC Requirements

NERC publishes a number of transmission planning standards that define the performance requirements the BESs in North America must meet, including single protection system failure contingencies. It is generally considered that protection systems should be able to clear all single-phase-to-ground and multiphase faults in a clearing time such that the system remains stable (including system voltage stability), facility ratings are not violated, and elements beyond the normal backup zone are not tripped [9].

In cases where delayed fault clearance is acceptable (such as those initiated by time-coordinated local or remote protection elements), it is possible to allow local backup protection elements to clear faults within the zone. For most BES-impactive circuits, however, instantaneous protection is required to be unavailable in at least one of the two protection systems in order to meet the stability requirements for the overall power system. Should high-speed/instantaneous tripping be available in both the protection systems, violating the allowable clearing time criterion, then an operator action must be taken to remove the associated power system element from service.

C. Example Utility Practice

The transmission system within the province of Ontario, Canada, operates at three voltage levels (500, 230, and 115 kV) and is further subdivided into two groups: impactive and nonimpactive. The impactive nature of a circuit is determined by its ability to adversely affect the Northeast Power Coordinating Council (NPCC) interconnected grid. For those elements considered impactive, fully redundant protection systems (A and B systems), with dedicated ac sources, dc circuitry, and power supplies, and communications channels are provided to ensure that a single contingency failure in any one protection system still allows for instantaneous fault clearance.

Each protection system on impactive lines includes a zone instantaneous (ZI) trip path and zone timed (ZT) trip path. The ZI path is usually either a pilot-assisted distance scheme (permissive overreaching transfer trip [POTT] or directional comparison blocking [DCB]) or 87L with an associated transfer trip and is intended for instantaneous fault clearance with an associated autoreclose attempt. The ZT path is used for local backup tripping only (no reclose) and is asserted from either of the following:

- An inverse-time zero-sequence overcurrent element (to prevent nearby generator unbalance protection [e.g., negative sequence] from operating for low-current open-phase conditions on HV lines) with a minimum tripping time of 1 second.
- A 400-millisecond timed trip from the overreaching Zone 2 distance elements (phase or ground), regardless of the status of the associated pilot signal.

Two possible cases are considered for the loss of instantaneous tripping in a given system. The first case is a complete failure of the protection itself (e.g., as annunciated by a critical failure alarm contact), where no trip (instantaneous or delayed) is expected from the given system. The second case is the situation where only a delayed trip is possible, such as in the event of a communications channel failure in a POTT distance or line current differential scheme. In the event of a loss of instantaneous tripping for an impactive element in both A and B systems, the operators are forced to take action to remove the element from the power system, even if time-delayed backup protection is still available in at least one of the two systems. In the case of nonimpactive circuits under the same conditions, the circuit is also removed from service, unless removing it has an adverse impact on customer load.

IV. GENERAL 87L BACKUP AND REDUNDANCY CONSIDERATIONS

Instantaneous and selective tripping for all line faults requires communications. As a result, channel availability impacts protection availability and the functional requirement of fast fault clearing times.

A. Channel Redundancy for Communications-Based Schemes

Channel redundancy is the preferred solution to maintain high availability for DC schemes. These schemes use a simple on/off type of signaling (permission or blocking) and therefore can be applied over low-bandwidth channels ranging from power line carrier and analog microwave through teleprotection I/O in a synchronous optical network (SONET) system [10] to digital teleprotection signaling directly over DS0 SONET channels.

Channel redundancy is an option for maintaining high availability for 87L elements as well. However, this option is viable only in two-terminal applications because typical 87L relays support only two 87L ports and the associated hot standby logic is designed to switch between two channels connected to a single remote relay. In addition, the 87L channels need to meet more stringent requirements compared with DC channels [2] [3]. Therefore, obtaining a second set of completely redundant 87L channels can be more costly or technically less feasible as compared with obtaining a second channel for a DC scheme.

B. 87L Backup

87L backup is often applied instead of, or in addition to, providing for 87L channel redundancy. This solution is often preferred because it addresses all possible failure modes that render the 87L scheme unavailable (see Section II).

Backup elements are typically required to provide timed clearance for the entire line, preferably within stability limits. Additionally, backup protection can provide instantaneous fault clearance for part or all of the protected line (ideally without overtripping). This requirement can be satisfied using a DC scheme or Zone 1 extension logic.

To be considered for 87L backup, DC schemes require a channel independent of the 87L communications network. Such a channel may not be available in some cases where the utility has made a transition to SONET-based communications and decided to decommission all legacy communications (e.g., power line carrier, analog microwave, and leased lines). In some cases, however, an independent channel may be available, facilitating 87L backup with DC schemes (e.g., direct fiber for 87L schemes and power line carrier for DC schemes).

Time-coordinated backup for remote bus faults may be required as a part of a remote backup strategy (catering for a catastrophic situation at a station, such as a fire or dc battery failure, that makes a number of protection systems unavailable simultaneously), regardless of the need to back up the 87L elements. Time-coordinated backup may also be required to provide for the adequate sensitivity of protection, while ensuring selectivity.

Considering that the 87L backup is required only in rare cases when the 87L is not guaranteed to be available, requirements of speed, selectivity, and sensitivity can often be modified for the backup functions as compared with the 87L elements.

Available backup elements are reviewed in more detail in Section V.

C. Integrated Versus Standalone 87L Backup

Considering that the 87L backup covers failure modes related to 87L channels and external time sources (if used), it is acceptable to integrate the 87L backup elements within the same relay.

Failures of the relay as a whole are covered by the redundant protection system. If two systems are required to keep the line in service, either forced outages are accepted as an operating procedure or a triple-redundant protection system should be considered. Effectively, a standalone backup system for the 87L elements would amount to the third (at least partially independent) protection scheme but with additional installation, engineering, and maintenance costs.

Most 87L multifunction relays allow for a wide range of backup functions that could be enabled or controlled to fulfill different backup protection philosophies.

V. BACKUP ELEMENTS FOR 87L SCHEMES

This section describes protection elements available to protection engineers to back up the 87L elements. This section is not concerned with whether these elements are integrated in the same device or not. The backup elements are listed in order of their overall performance.

A. Directional Comparison

The DC scheme is typically composed of a combination of distance elements (21P/21G) and/or directional elements (67P/67Q/67N). In this scheme, the direction of the fault as seen by each remote relay is compared to the direction of the fault as seen by the local relay. If the directional comparison agrees (i.e., the fault is internal), the scheme trips instantaneously. In order for the individual line relays to communicate their fault direction to each other, a communications channel is required; for backup protection applications, this communications channel needs to be independent from the communications channel used by the 87L element. If this is not the case and the 87L element becomes unavailable due to a communications channel-related issue, then the DC scheme also becomes unavailable.

The distance elements (21P/21G) and the phase directional element (67P) are intended to operate for high-current, low-resistance faults and are set to overreach the remote terminal(s). However, because each relay does not see the total fault current in the line (measuring only the local current contribution), the overall sensitivity and selectivity of the protection scheme may be lower than that of the 87L scheme.

The sequence directional elements (67Q/67N) are intended to detect high-resistance faults or low-current open-phase faults within the protected zone; however, as mentioned previously, because the relays at each terminal do not see the total fault current, the ability of a scheme to trip for high-resistance faults is diminished. Fig. 2 shows a system where one terminal of the line is fed by a strong source and the other terminal is fed by a weak source. Should a high-resistance fault occur on the line, the strong terminal will supply enough current to the fault to meet the minimum pickup threshold of the sequence directional element, whereas the weak terminal may not meet the minimum threshold and therefore a sequential trip of the faulted line may result.

Furthermore, if the 67Q/67N elements are responsible for keying signals in the DC scheme, correct phase selection cannot be guaranteed.

In general, a DC scheme is capable of creating a unit protection scheme but often does not provide the same sensitivity, selectivity, or speed as an 87L scheme.

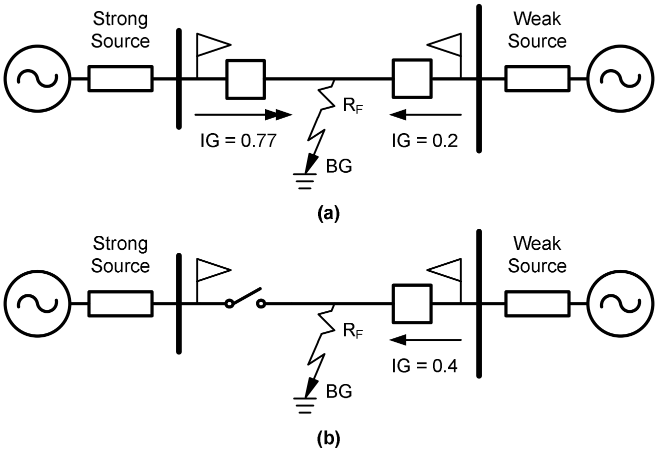

Fig. 2. A high-resistance fault fed from a strong and a weak source, respectively. As long as the strong source is connected, the weak source may not supply enough fault current to enable the directional element (a). When the strong source is disconnected, the weak source can supply enough fault current to enable the directional element (b).

B. Zone 1 Extension Logic

When independent communications channels are not available and accelerated tripping for the remaining section of the transmission line not covered by a traditionally set Zone 1 element is desired, a Zone 1 extension scheme is a viable option.

When the local breaker closes, the Zone 1 reach is set at 70 to 80 percent of the line impedance (typical Zone 1 setting). Should the breaker remain closed for longer than a pre-set time, the Zone 1 setting is increased to 120 percent of the line impedance. This now affords instantaneous protection for the entire line at the expense of selectivity. If an external fault occurs close to the remote terminal, the local Zone 1 trips instantaneously, along with the remote terminal protection, as shown in Fig. 3a. However, this may not be a major concern if the sequence of overtripping and reclosing of lines is allowed because the local terminal would reclose and restore the unfaulted line to service. When the local terminal is tripped, the Zone 1 reach setting is returned to the preextension value (70 to 80 percent of the line impedance), as shown in Fig. 3b; this prevents the local relay from tripping should the out-of-section fault prove to be permanent.

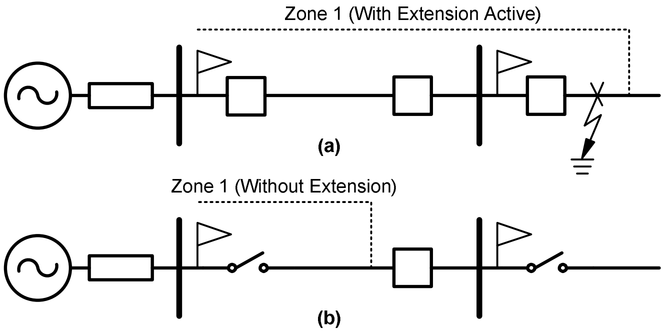

Fig. 3. Zone 1 reach for a Zone 1 extension scheme after the breaker has been closed for a predetermined time (a). Once the breaker opens, the Zone 1 reach is reduced (b).

Careful consideration needs to be given to the maximum allowable Zone 1 reach extension with regard to power swings and line loading and the application of power swing blocking and load-encroachment elements. In addition, the Zone 1 extension scheme may not be applicable at all for lines with series compensation (or lines adjacent to series-compensated lines) or for lines with tapped transformers (in order to reach short of the low-voltage bus).

C. Stepped Distance Backup

In stepped distance backup, Zone 1 is set per typical practices not to overreach the remote terminal (typical setting of 70 to 80 percent of the line impedance). This setting, however, leaves a portion of the line with no instantaneous protection. Therefore, a set of time-delayed elements is needed to protect the remaining portion of the line. Typically, Zone 2 elements are set at a minimum of 120 percent of the line impedance, but if the line has multiple infeeds or is feeding a bus with multiple lines connected to it, the Zone 2 reach can be set larger than 120 percent of the line impedance. The reason for this setting is that the effect of infeed from the other terminals or adjacent lines (such as for the external faults shown in Fig. 4) results in an increase of the apparent impedance and therefore in underreaching of the local Zone 2 distance elements. This means that the ability of a Zone 2 element to see faults is reduced, thereby also reducing the ability of the Zone 2 element to trip for out-of-zone faults. This also, unfortunately, impairs the role of Zone 2 as a remote backup for out-of-zone faults.

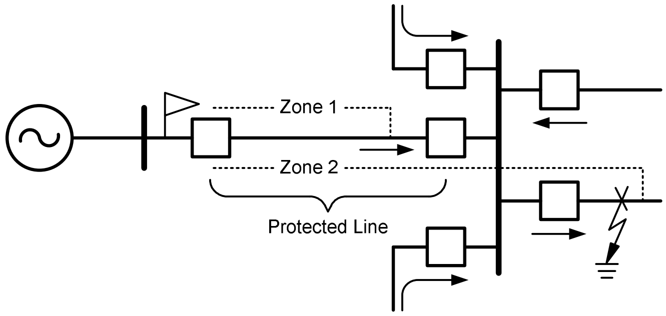

Fig. 4. Infeed from the adjacent lines reduces the effective reach of the Zone 2 element.

Because the aim of the Zone 2 elements in this scheme is to provide protection for the portion of the line not protected by the instantaneous Zone 1 element, Zone 2 needs to operate as rapidly as possible without adversely affecting the selectivity of protection (if possible) or the reliability of the power system. The typical delay of the Zone 2 element is 20 to 30 cycles (333 to 500 milliseconds); in this case, the Zone 2 element should operate faster than this but not before the remote breaker failure time (on the order of 6 to 12 cycles or 100 to 200 milliseconds). Therefore, the time delay of the Zone 2 element is set to include the remote breaker failure clearing time plus a margin (on the order of 12 to 15 cycles or 200 to 250 milliseconds). This time is long enough to prevent the remote-end relay(s) from tripping for faults close to the terminal but, at the same time, provide backup protection should the remote primary scheme fail.

It is important to note that both the Zone 1 and Zone 2 elements are only intended to detect high-current (low-resistance) faults. For the detection of high-resistance faults and low-current open-phase faults, these elements need to be supplemented by negative- or zero-sequence time-overcurrent elements. Furthermore, the same considerations must be made as with the Zone 1 extension scheme with regard to power swings, line loading, series compensation, and tapped transformers.

D. Time-Overcurrent Backup

One final option for backup protection is the use of time-overcurrent elements, operating on either phase currents or sequence currents.

However, using time-overcurrent elements can prove to be very challenging. The magnitude of the fault current varies with the fault location, the fault resistance, and the strength of the source behind the relay. Furthermore, basic time-overcurrent elements lack the ability to determine the direction of the fault. It is possible to solve this problem by supervising (torque-controlling) these elements with a directional element. Additional consideration for phase-overcurrent elements must be made for heavy load conditions, line energization, and power swing conditions.

Time-overcurrent elements that operate on either negative- or zero-sequence current are intended to detect high-resistance faults or low-current open-phase faults on the line, so their pickup value is typically set very sensitively. Because these elements should not operate before any of the main protection elements nor should they operate before any adjacent backup protection for external faults in an adjacent zone, these elements must have a time delay that adequately coordinates with the protection in adjacent zones. Further consideration needs to be made in single-pole tripping applications (similar to that in the DC scheme).

In general, when time-overcurrent elements are used as backup protection, they should only detect high-resistance faults or low-current open-phase faults on the line, where the fault does not immediately threaten the stability of the power system, while ensuring such faults are cleared prior to miscoordination with generator protection throughout the system.

VI. LINE CURRENT DIFFERENTIAL BACKUP STRATEGIES

As discussed previously, backup protection may be implemented either in the primary relay itself (particularly in the case of a multifunction microprocessor-based relay) or in separate, standalone relays. Reference [11] provides a sound methodology to select and analyze the reliability of redundant systems. In this paper, we simply include general considerations without rigorous analysis of reliability and availability.

A. Fully Operational Backup Scheme in Parallel With 87L

One option for providing backup protection to line current differential elements is to apply a completely functional set of backup protection elements that run continuously in parallel with the primary differential function. For this type of strategy, the backup protection can either be integrated into the primary differential relay or just as easily implemented in a separate relay (or set of relays). In this solution, the backup protection does not require any knowledge of the status of the primary differential protection function in order to provide backup protection.

In this option, the backup protection scheme is biased strongly towards dependability (two schemes in parallel). The tradeoff is that the backup protection is biased away from security, relying on settings and time coordination in most cases rather than the inherent selectivity and security of the main differential function. In cases where normally operating differential protection would otherwise restrain and not trip, miscoordination may result in an undesired overtrip.

If the backup elements are effectively single-ended (e.g., overcurrent and stepped distance) and therefore typically less secure when compared with the 87L element (e.g., during power swings), allowing the backup to be operational even with the 87L intact may be disadvantageous if security is of paramount importance.

B. Backup Scheme Engaged Only Upon Loss of 87L

Additional security can be provided for backup protection schemes by enabling the backup protection elements only when the 87L element has explicitly been declared to have failed or when a single contingency may adversely affect the availability of the 87L function (see Section II). For example, a three-terminal 87L scheme may enable the backup elements in the event of a single channel communications failure that results in a given terminal operating in a slave mode (i.e., having one of the two communications channels unavailable [see Section II]). By enabling the backup elements only when the main differential protection is unavailable, the backup scheme will not be exposed to overtripping under normal circumstances where the inherently selective differential protection can reasonably be expected to restrain correctly for external faults and trip correctly for internal faults.

Consider the situation where a three-terminal differential scheme is operating in the master-slave mode due to a prior communications contingency (e.g., maintenance outage on the communications infrastructure [see Section II]). There are two possible options for enabling the backup protection scheme (assuming that a phase and ground distance 21P/21G scheme is used).

In the first application option, the timed distance backup scheme is enabled only in the case of a complete loss of 87L functionality (dual channel failure).

In the second application option, the distance backup is enabled with the first communications channel contingency (i.e., local 87L terminal operating in the slave mode).

When using the first option, the backup protection elements must wait for the primary 87L function to declare that it has failed before they are allowed to pick up and start timing. This may result in the backup elements taking even longer than expected to operate due to having to wait for the 87L failure to be declared; in the event of an intermittent problem in one channel, there may be an extremely delayed trip or failure to trip. Therefore, it may be beneficial to have an instantaneous underreaching Zone 1 enabled at all times.

When using the second option, where the backup protection is armed on the first communications contingency, the backup protection tripping time is as intended with no additional delay (including instantaneous tripping, if implemented). In the event of a fault, the backup elements pick up immediately and start timing out so that they will operate at the intended time in order to clear the fault before any adjacent backup protection elements operate.

There is always the possibility in either of these cases of the backup scheme incorrectly tripping for external faults due to the loss of the inherent selectivity of the differential protection. However, the likelihood of such overtripping is greatly reduced by having the backup scheme operational only under contingencies. When the backup elements are enabled only for a complete failure of the primary differential function, the scheme is biased for security at the expense of dependability and speed. When the backup protection elements are enabled on the 87L scheme being suspect rather than obviously failed, the scheme is biased more towards dependability and maintains speed at the expense of security.

C. Adaptive Backup Schemes

One primary advantage of using modern microprocessor-based relays for differential protection is the ability to use the internal programmable logic and multiple settings groups to deal with different operating conditions and contingencies related to the primary differential scheme. For example, an extension of the instantaneous tripping Zone 1 scheme discussed in Section IV can now be implemented, whereby the actual backup scheme can dynamically be changed depending on the overall availability of the primary differential element to tailor the backup scheme to improve dependability and provide instantaneous fault clearance.

Consider a three-terminal application, for example. In the normal operating case where all three terminal relays and all three communications links are functioning normally, the differential element can be relied upon to detect all internal faults and to correctly restrain for all external faults. In this case, the settings group and user-programmable scheme logic should decide to use only the differential element for protection tripping. In this configuration, only the differential element would be enabled; the backup protection elements would be disabled or otherwise prevented from picking up (e.g., through the use of a torque-control equation). Now, assume that a single communications contingency impairs the differential function for two of the relays and, as a result, these relays must now rely on a transfer trip from the differential element running in the master terminal relay in order to clear an internal fault. In this case, it would be advantageous to enable backup protection, as discussed previously.

Most modern microprocessor-based line current differential relays provide at least two elements for both phase and ground distance protection, in addition to the primary differential element. These elements can be used to provide backup protection with a high degree of dependability and security for both single and dual contingency events. One major advantage of tailoring the backup scheme based on the operating configuration is that additional nondelayed elements can be enabled, which allows the associated line to reclose for obvious internal faults. Even in the event of an overtrip of an instantaneous element, the protected line should successfully reclose and restore the circuit to the prefault state.

In the case of a single contingency event, the underreaching Zone 1 elements could be enabled and set to protect roughly 80 percent of the line in a two-terminal line (Fig. 5) or the entire segment between the terminal and the tap point in a three-terminal line (Fig. 6). By setting the Zone 1 elements in this manner, a high-speed trip can still be obtained in the slave relays even in the event of the master 87L terminal being in the stub bus configuration (i.e., isolated from the line by an open disconnect [see Section II]) by cascading transfer trip signals between the two slave terminals via the master. The Zone 2 elements in the slave relays can be set to overreach the remote terminals with a fixed long time-delay setting, typically set greater than the remote terminal fault clearing time, including breaker failure.

In the case of a dual contingency communications failure or in situations where 87L is otherwise explicitly declared unavailable, the backup protection could be dynamically modified (e.g., using settings groups) to extend the reach of the instantaneous Zone 1 distance elements and reduce the time delay for the operation of the Zone 2 element.

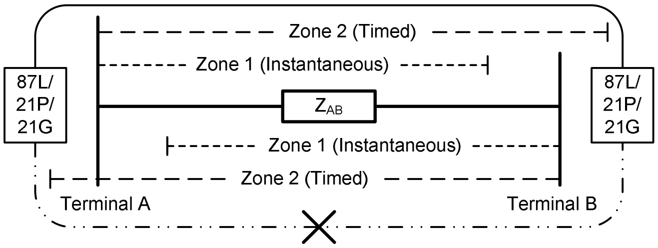

Fig. 5. Distance backup strategy for two-terminal lines based on instantaneous underreaching Zone 1 and overreaching time-coordinated Zone 2.

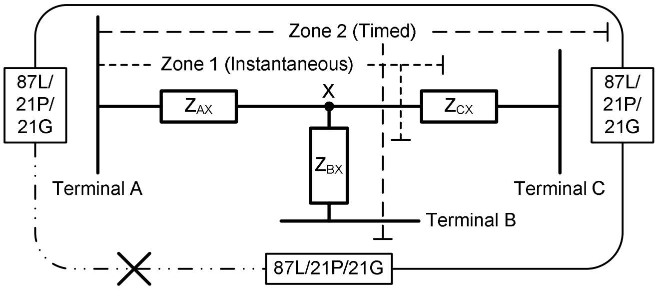

Fig. 6. Distance backup strategy for three-terminal lines based on instantaneous Zone 1 overreaching the local line segment and time-coordinated Zone 2 overreaching both remote terminals.

In a three-terminal line (Fig. 7), the Zone 1 instantaneous element at Terminal A could be extended to cover the segment to the tap plus some additional percentage of the adjacent segments. For example, the Zone 1 reach at Terminal A could be set with REACH = $Z_{AX} + 0.8 \bullet \min(Z_{BX}, Z_{CX})$ in order to cover as much of the line as possible while still underreaching the closest terminal in the case where one terminal is open (the three-terminal line operating as a two-terminal line). This reach setting would allow for a higher dependability for instantaneous tripping while still being secure against tripping instantaneously for external faults (in three-terminal situations, the infeed effect would additionally cause the Zone 1 instantaneous element to underreach for faults beyond the tap).

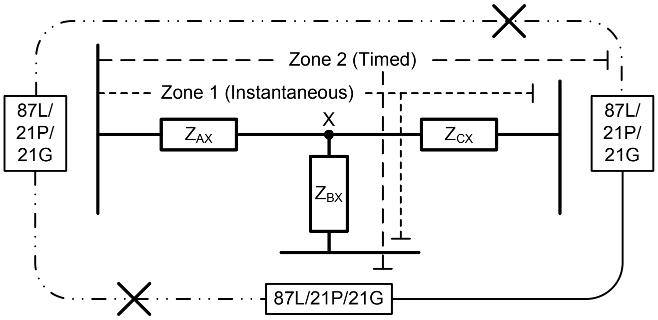

Fig. 7. Distance backup strategy for three-terminal lines based on instantaneous Zone 1 overreaching the tap point as much as possible but set short of the closest remote terminal and time-coordinated Zone 2 overreaching both remote terminals.

The Zone 2 element could be configured to remain the same, or alternatively, the time delay applied for this contingency could be reduced to the normal maximum remote clearing time (not including breaker failure) plus a margin. This setting would allow higher-speed clearance for internal faults beyond the Zone 1 reach, thus potentially preventing miscoordination and overtripping of adjacent zone backup protection schemes due to slow fault clearance. The tradeoff is, of course, security, in that the Zone 2 (short) timed backup elements can overtrip in the event of a slow fault clearance in an adjacent zone.

D. Stub Bus Configuration Considerations

Additional logic can be provided to deal with stub bus configurations, where a modified DC scheme could optionally be enabled at the stub bus end. A permissive signal received over the communications channel from each slave relay (e.g., keyed from Zone 2 pickup) could be connected by AND logic with the local stub bus status in the master relay. Should permissive signals be received from both slave relays, then the master could send a corresponding DTT signal to the slave relays. The slave device, upon receiving the DTT signal, would then trip instantaneously.

Additionally, the Zone 1 backup protection elements in one of the slave terminals used to trip the local breakers could also be used to send an additional transfer trip over the remaining healthy 87L communications channel to the master relay. The master relay could cascade the signal to the other slave terminal to trip those remote terminal breakers as well (Fig. 8). This is also useful in cascading a local breaker failure trip signal to the remote terminal. Note that a separate DTT must be used for the purposes of cascading, in order to prevent the trip from latching up in the event of a fault when all three communications links are operational.

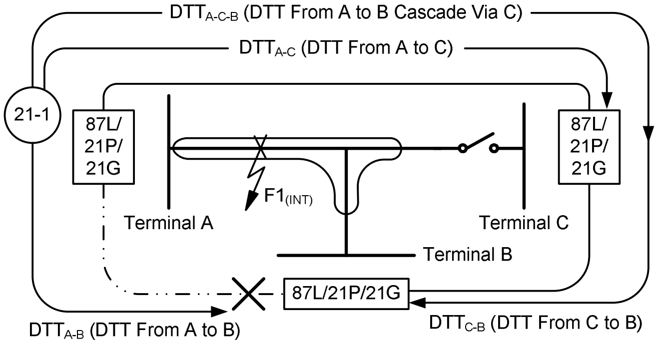

Fig. 8. Master relay used to cascade DTT between slave relays.

The overall logic for this application is shown in Fig. 9.

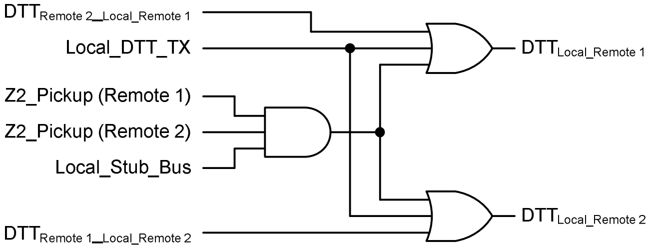

Fig. 9. DTT logic catering for master-slave configuration where the master relay is in a stub bus configuration.

VII. Selecting Communications Paths

This section discusses some basic considerations for selecting communications paths for line current differential protection. Particular attention is given to Hydro One Networks, Inc. (HONI) practices. In general, the approach described here focuses on providing maximum redundancy of communications within each protection system, rather than counting on self-healing capabilities of the communications network.

Historically, traditional communications-based distance schemes have relied on analog communications systems between stations. In modern installations, the two most common options for analog communications channels have been power line carrier and leased analog voice frequency circuits. In the case of power line carrier applications, where the communications are carried over the associated transmission line (or a parallel circuit on the same right of way), the communications infrastructure is owned and maintained by the utility. For voice frequency circuits that are leased from a local telecommunications provider, there can be significant long-term operating costs and the communications infrastructure is predominantly outside the control of the utility.

For modern digital differential relaying, a digital communications infrastructure that provides adequate bandwidth, low BER, and tolerable (and symmetrical) delays is an absolute requirement in almost all cases. When digital line current differential protection is applied in at least one of the protection systems, the communications are forced to be digital only and usually implemented over the SONET [10] infrastructure (possibly integrating digital microwave communications). In these cases, and especially where line current differential protection is applied in both protection systems (A87L and B87L), the choice of communications infrastructure used to implement the protection schemes faces fundamental constraints. Implementing the necessary digital communications infrastructure for digital current differential protection requires a large initial capital investment (along with considerations for technology obsolescence of the digital infrastructure). Therefore, it is generally unlikely that a separate independent analog communications infrastructure (power line carrier, analog leased facilities) will be installed and/or maintained as well.

The challenge becomes providing a reasonable amount of communications redundancy and diversity between redundant protection systems. Under ideal circumstances, complete redundancy would be provided between protection systems, including the following:

- Separate DS1 access multiplexers (if used).
- Separate SONET multiplexers.
- Separate SONET rings for unique main and alternate routes for both protection systems.

This arrangement, while being ideal in terms of reliability, would be prohibitively expensive and face significant long-term maintenance and end-of-life replacement costs. An added limitation is that there are usually only a fixed number of geographically diverse paths that any SONET infrastructure can use between two stations before considerations have to be made regarding channel latency when sending data over too long a distance for the sake of path diversity. It is necessary therefore to find a reasonable compromise to allow generally fault-tolerant communications infrastructure within the economic and geographic constraints of a given utility. One scheme typically used with line current differential applications over SONET is shown in Fig. 10.

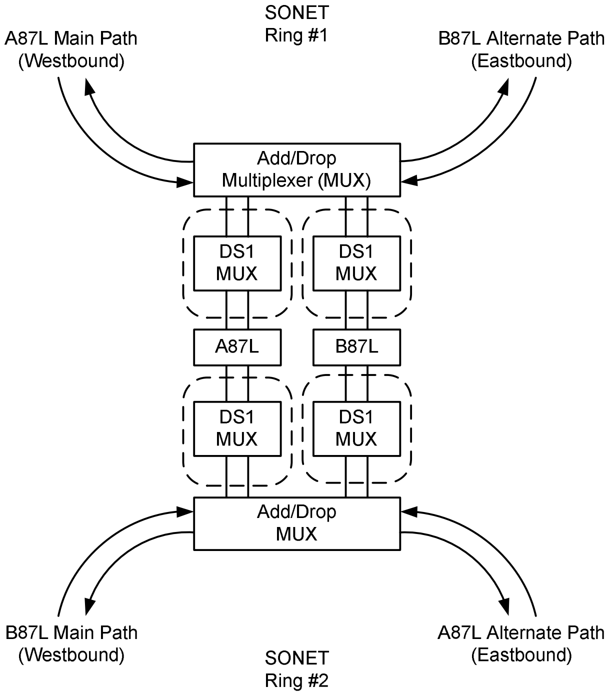

Fig. 10. Completely redundant and independent communications for dual-redundant communications-based protection systems.

This arrangement allows for a single communications failure to occur, while still preserving the overall ability of the protection schemes to remain functional. Most single communications failures only impact the normal operation of one of the two redundant protection systems. The exception is the complete failure of a SONET add/drop multiplexer, which would introduce a single communications failure into both protection systems. However, because most line current differential schemes are fault-tolerant for single communications failures, this should not cause any adverse impact on protection performance or availability.

For DC schemes, if the pilot (and transfer trip, where applied) signals are keyed using discrete I/O and hard-wired connections (which is the case in HONI current applications), the number of redundant paths is limited only by the amount of physical I/O in the distance protection scheme and the total number of diverse communications paths available (both digital and analog).

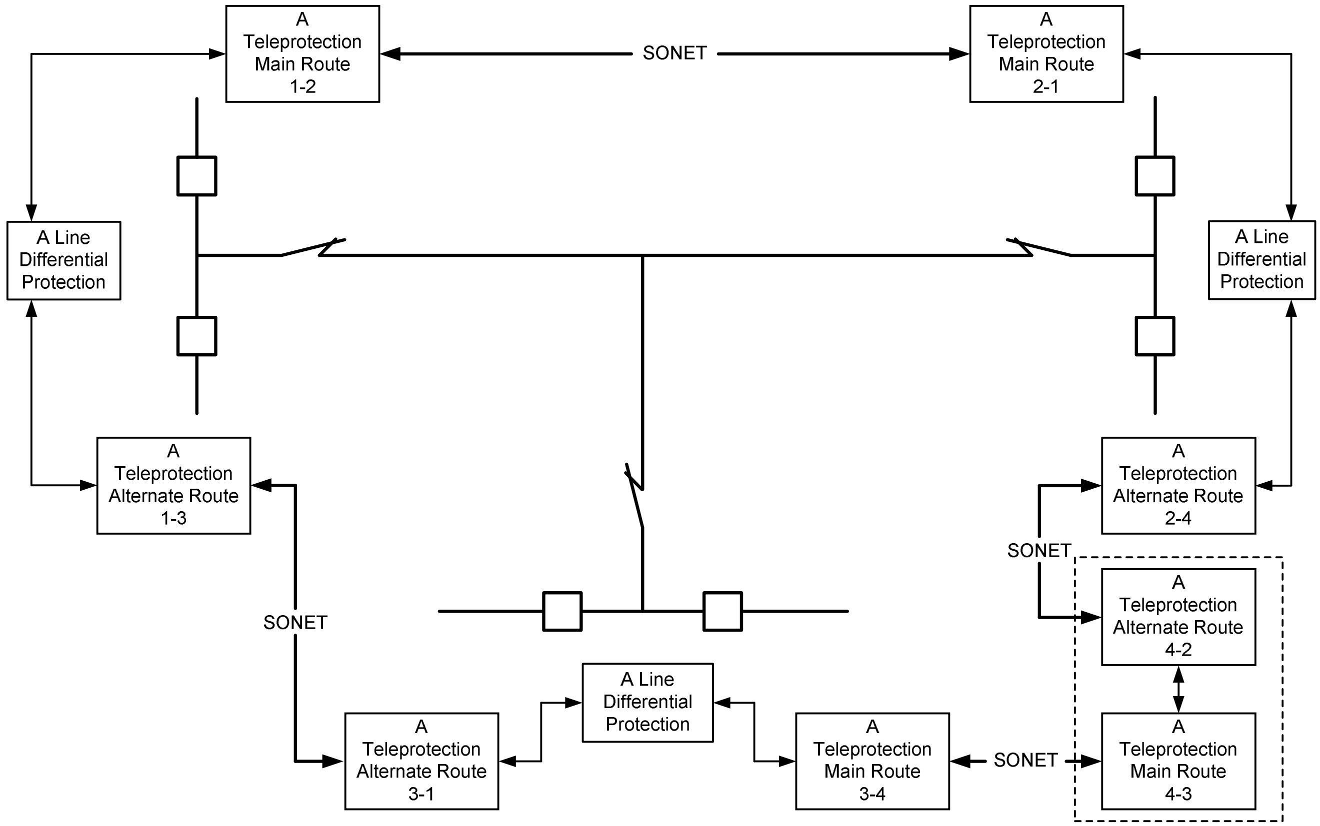

Fig. 11. Three-terminal 87L application with two SONET rings crossing over at the fourth location (even though the Group A system is shown, the Group B system follows the same approach).

For line current differential protection and, in particular, applications for three-terminal lines, the choice of communications architecture is essentially limited by the fact that most existing line current differential relays only support two 87L communications ports. The end result is the typical communications architecture for three-terminal line current differential applications, as shown in Fig. 11. Note that in the three-terminal line current differential application, there may be a fourth terminal required, where a crossover between SONET rings (usually made at the OC-3 [10] level) is created to route the communication for the third communications path.

Providing such communications architectures requires some careful considerations. The first consideration is geographic diversity, where ideally both paths of the communications infrastructure will not be geographically concurrent with the associated protected line. This, however, is not generally the case because often one of the paths is contained in an optical ground wire (OPGW) running along the same (or nearby) set of towers carrying the protected line. In this case, should the OPGW break, it may come in contact with the protected line as it falls, resulting in a near-simultaneous communications failure and fault on the associated line.

The other, and arguably more serious, consideration is the nature of the provision of the channels in SONET with regard to dynamic reconfiguration of the SONET communications paths. In the case of the HONI SONET system, all of the communications paths for protection applications (regardless of DC or differential) are static (pinned). In other words, path switching is not allowed for these circuits, and in the event of a failure of a given path, the path remains unavailable until it is repaired. This is done for the following main reasons:

- Implementing a path-switching scheme introduces added complexity, making explicit channel testing and prediction of overall system behavior difficult [4], especially as the size of a SONET system increases.
- All schemes, including line current differential schemes, continue to function with a single communications failure; therefore, the communications scheme is kept as simple as possible to maintain functionality in the event of a single contingency.
- Given that line current differential schemes are dependent on the stable and symmetrical behavior of their communications channels (unless using external time reference, which is not HONI standard practice), path switching can introduce unexpected changes to the communications channel that can actually lead to differential protection misoperations [12].

VIII. CONCLUSION

Line current differential protection is an inherently selective, sensitive, and secure protection scheme. Relying on communications and, in some cases, on external time sources, it needs to be properly engineered to cover communications or time source failures. This extra engineering effort is the main tradeoff versus the excellent security and simplicity in protection settings selection.

A variety of conditions related to communications and timing can render the 87L elements unavailable. In many cases, a single failure does not necessarily lead to the loss of 87L protection because some applications incorporate a certain degree of ride-through ability and provide for a fallback response. It is beneficial to understand the exact failure modes in communication and timing of a given application before selecting a backup strategy.

Considering that the 87L backup covers failure modes related to 87L channels and external time sources (if used), it is acceptable to integrate the 87L backup elements within the same protective device. Most 87L multifunction relays allow for a wide range of backup functions that could be enabled or controlled to fulfill different backup protection philosophies. This includes stepped distance, Zone 1 extension, overcurrent, and DC schemes. These solutions typically do not perform as well as the 87L scheme or require more effort to engineer them properly.

Regulatory requirements and internal practices impact the selection of the backup schemes for the 87L elements. Section III reviews typical requirements and practices.

Two major backup philosophies can be considered: parallel backup and backup engaged only upon problems with the 87L elements.

If the backup elements are effectively single-ended (overcurrent and stepped distance) and therefore less secure when compared with the 87L element, enabling the backup only when the operation of the 87L protection may not be ensured can be advantageous if security is of paramount importance.

Multifunction microprocessor-based relays allow adaptive backup schemes where the backup elements are enabled or controlled in response to the present status of the 87L elements. Section VI describes several such practical schemes.

Selecting communications paths for both 87L and DC schemes affects the overall availability of protection. Section VII presents one practical approach to provisioning DS0 SONET channels for protection applications.

IX. 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] 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.

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

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

[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] 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.

[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] IEEE Power System Relaying Committee Working Group I-19, *Redundancy Considerations for Protective Relaying Systems*. Available: http://www.pes-psrc.org.

[9] NERC System Protection and Control Task Force, "Protection System Reliability – Redundancy of Protection System Elements," November 2008. Available: http://www.nerc.com/docs/pc/spctf/Redundancy_Tech_Ref_1-14-09.pdf.

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

[11] E. O. Schweitzer, III, D. Whitehead, H. J. Altuve Ferrer, D. A. Tziouvaras, D. A. Costello, and D. Sánchez Escobedo, "Line Protection: Redundancy, Reliability, and Affordability," proceedings of the 64th Annual Conference for Protective Relay Engineers, College Station, TX, April 2011.

[12] NERC, "Lesson Learned – Phase Comparison Relay Protection Systems – Channel Delay," October 2010. Available: http://www.nerc.com/files/LL-Phase-Comp-Relay-Protect-Channel-Delay.pdf.

X. BIOGRAPHIES

Steven Hodder received a bachelor of engineering degree (first class standing) in electrical engineering from Lakehead University in Thunder Bay, Ontario, in 2000. He has over ten years of experience in the power system protection and control field and is currently a senior protection and control specialist in the engineering standards and new technology development department of Hydro One Networks, Inc., specializing in transmission and substation protection design. Steven is a member of the IEEE Power and Energy Society (PES) and Standards Association (SA).

Bogdan Kasztenny is a principal systems engineer in the research and development division of Schweitzer Engineering Laboratories, Inc. He has over 23 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. Normann 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.

Previously presented at the 2012 Texas A&M
Conference for Protective Relay Engineers.

20120425 • TP6546-01