Dependability Versus Security: Finding a Reasonable Balance

Jeffrey M. Pond and Yujie Irene Lu
National Grid

James E. Mack
Schweitzer Engineering Laboratories, Inc.

Presented at the
64th Annual Georgia Tech Protective Relaying Conference
Atlanta, Georgia
May 5–7, 2010

Originally presented at the
36th Annual Western Protective Relay Conference, October 2009

Dependability Versus Security: Finding a Reasonable Balance

Jeffrey M. Pond and Yujie Irene Lu, *National Grid*
James E. Mack, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—An age-old battle has been raging since the first electrical distribution system was installed. How sensitive do we set protective relays to be assured all faults are detected and isolated without risking overtrips? Overtrips isolate parts of a system more often than necessary, causing increased outages and potentially risking system stability. Conversely, an overly secure protection system may not detect some faults, leading to equipment damage. Typically, when a utility experiences a failure to trip, the relay sensitivity is increased. Several years may pass without incident, and then the line experiences an overtrip. After an initial analysis of the events, there is a tendency to undo the decision to increase sensitivity in favor of more security. This scenario begins yet another cycle of dependability versus security.**

With today's multifunctional protective relays, powerful protection schemes can be realized that provide the relay engineer with the capability to achieve both dependability and security without compromising either. However, the typical practice when these new systems are installed is to copy the electromechanical protection settings and schemes, especially if these are the standards for that utility. There is a prevailing mindset to not change these schemes and standards; however, to achieve increased dependability and security, we must step outside of our protective box.

When properly designed, today's protection systems provide better performance than electromechanical protection systems. For example, line protection schemes such as POTT (permissive overreaching transfer trip) and DCB (directional comparison blocking) have evolved into hybrid versions. With high-speed, inter-relay communications combined with many new and advanced relay elements, the relay engineer has an opportunity to further improve these schemes, which was not possible with electromechanical relays. Improvements include combining the best features of several schemes, adding direct tripping for close-in faults, setting separate timers for fast and delayed tripping on DCB schemes, and adding additional supervisory permissives, such as undervoltage elements, to allow the signal to echo back. This paper delves into applying new modifications to age-old proven schemes and then analyzes the potential benefits, enhancing dependability, security, or both.

I. Transmission Line Protection

Relatively speaking, transmission protection schemes have not evolved greatly over the past 50 years. Modern relays facilitate the development of newer protection schemes and the modification and resulting improvement of tried-and-true protection schemes. Protective relays now have enough logic capability to allow the user to build any standard scheme, modify standard schemes, or build entirely new protection schemes.

Communications systems have come a long way in the past 50 years, and they can now have a profound impact on transmission system protection. Microwave and fiber optics provide the necessary bandwidth for the design of more advanced protection with multiple I/O channel capability and the transfer of fast analog data across the system.

The following is a discussion of standard protection schemes, modifications to those schemes, and some new protection schemes and the relative dependability and security they provide.

A. Permissive Protection Schemes

POTT (permissive overreaching transfer trip) is the most widely used protection scheme in the permissive trip category. This scheme traditionally uses forward overreaching phase and ground zone distance elements to key permission for the remote end to trip, conditional that the remote-end forward overreaching element is also picked up. With both ends of the line protection pointing forward, the reasoning is that the fault must be on the protected line section. Overreaching mho distance elements ensure all zero-impedance faults on the line section are seen by the element. Traditionally, the set reach has been 120 to 150 percent of the impedance of the protected line section, providing moderate coverage for ground faults with impedance (Fig. 1).

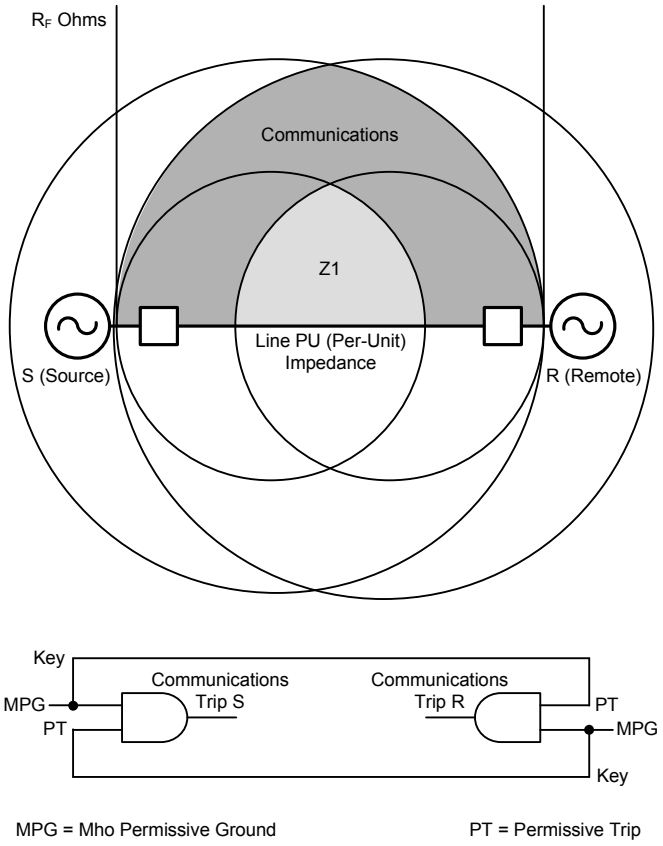

Fig. 1. POTT with mho elements

More coverage for high-impedance ground faults can be obtained by increasing the reach to many times the line impedance, at the risk of decreasing security (Fig. 2).

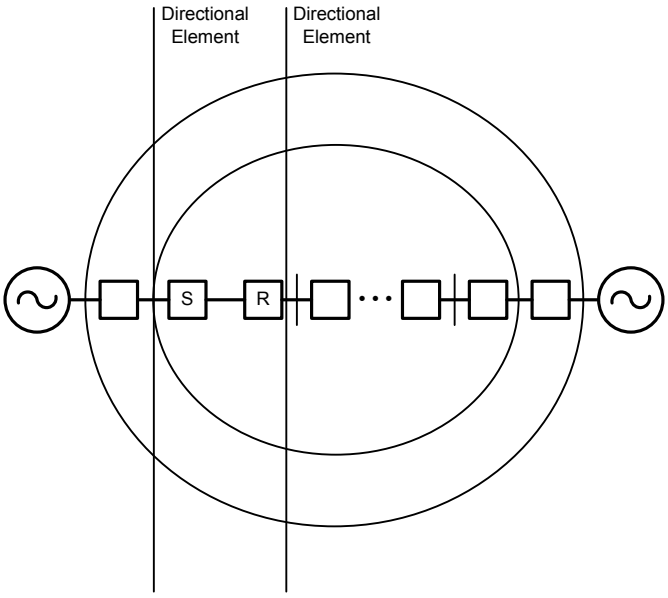

Fig. 2. Breaker S mho element set to six times line impedance, and Breaker R mho element expands back to remote source

As an alternative, quadrilateral distance elements can be added with significant resistive reach while maintaining the traditional 120 to 150 percent line coverage and preserving the inherent security in the protection scheme (Fig. 3).

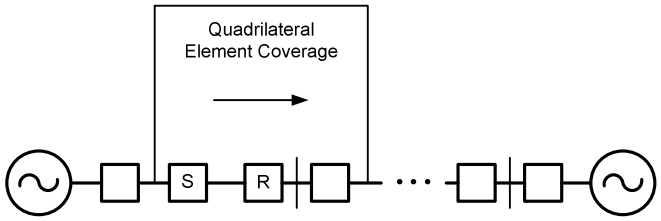

Fig. 3. Quadrilateral elements provide better resistive fault coverage where mho expansion is not possible

In recent years, it has become popular to add low-set forward directional ground and/or negative-sequence directional overcurrent elements to provide very sensitive and high-impedance fault coverage. Very sensitive elements are also more likely to see faults at weak terminals or terminals that see very high apparent impedance (Fig. 4).

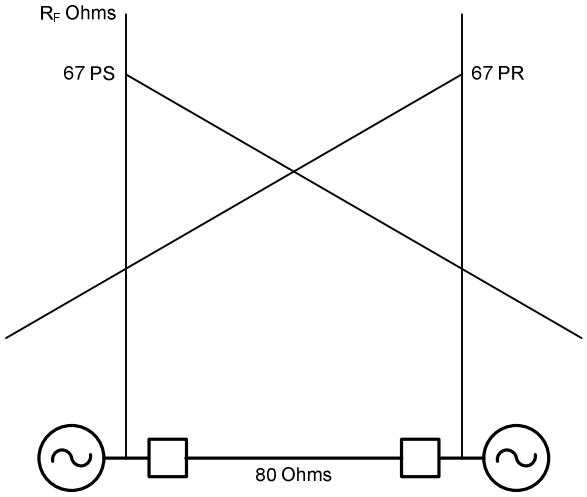

Fig. 4. Sensitive permissive overreaching ground overcurrent element

These low-set directional ground and negative-sequence directional overcurrent elements cause some reduction in security with the advantage of significantly increasing dependability.

The POTT scheme in its pure form does not allow sequential clearing on lines that have weaker terminals or terminals that see high apparent fault impedance. This is a major limitation in dependability of the pure POTT scheme. Sequential clearing takes place when the stronger terminal is allowed to trip first because the weaker terminal or terminals do not see the fault. After the stronger terminal clears, the system transfer impedance normally presents a stronger source at the terminal that does not see the fault, moving the fault impedance into the element range to allow fast tripping.

This leads us into the first, most popular hybrid derivation of POTT, echo back (Fig. 5).

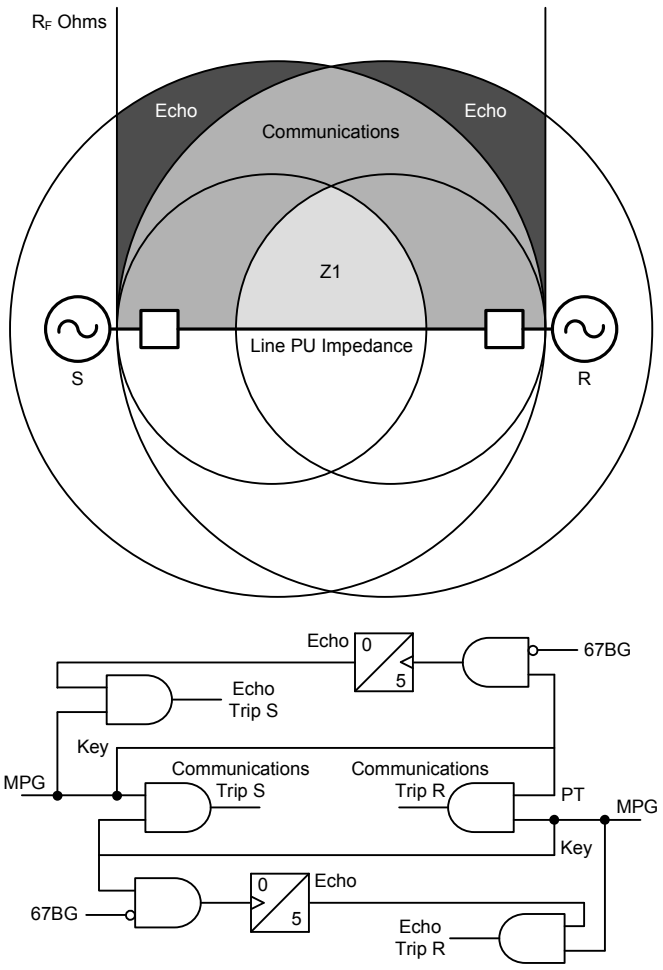

Fig. 5. POTT with mho elements and echo logic

Adding echo-back functionality to POTT allows the permissive signal to be echoed back to the original sending terminal, as long as the echoing terminal does not see a reverse fault. This allows sequential clearing in a very similar manner to the DCB (directional comparison blocking) scheme that will be discussed later. The echo feature requires that the relay engineer properly coordinate the forward-reaching permissive element with the remote-end reverse-reaching blocking element (i.e., the reverse element blocks an echo back from occurring). This coordination is very crucial in maintaining security. This important concept can be visualized on R-X impedance diagrams. Fig. 6 shows POTT with overreaching ground mho elements coordinating with a reverse-reaching ground directional overcurrent element.

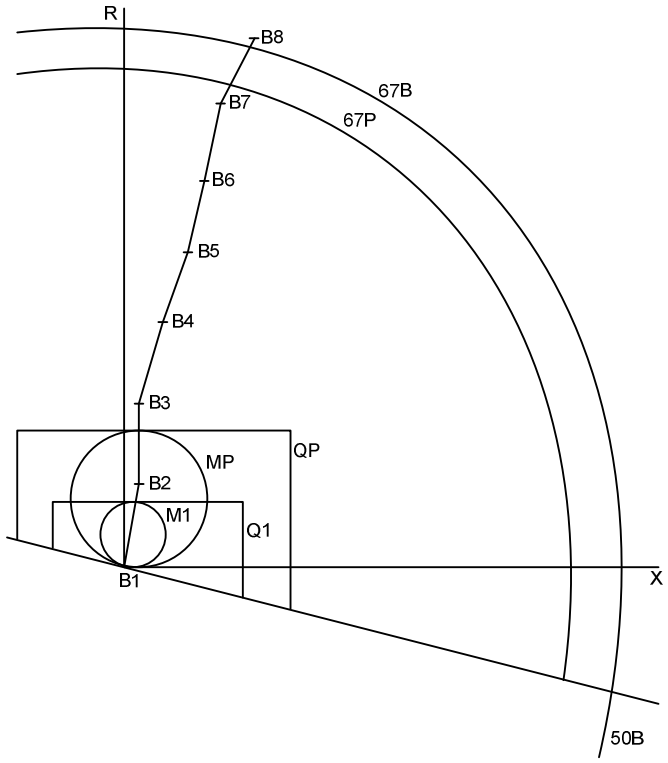

Fig. 6. R-X impedance diagram visualization of low-set directional overcurrent coordination challenge

This is a very secure coordination, plainly evidenced by the area of impedance coverage by each element on the R-X diagram. Fig. 6 shows a ground quadrilateral element easily coordinating with a reverse directional overcurrent echo-blocking element. Fig. 6 also shows the risk of attempting to coordinate the low-set forward directional overcurrent permissive element with the remote-end echo-blocking reverse directional overcurrent element. Please note that a directional ground overcurrent element set at 0.5 A reaches 1,000 miles or more at 230 kV and above. Many utilities do utilize this scheme to achieve fast clearing for high-impedance faults anywhere on the line and accept the risk of overtripping.

Memory-polarized elements are the prevalently used elements because of their desirable expansion qualities to provide more sensitive ground fault coverage for higher impedance faults. Mho element expansion is a major consideration when deciding whether to use ground directional overcurrent elements. On longer lines with stronger sources, the memory-polarized mho element will not expand very much (Fig. 7).

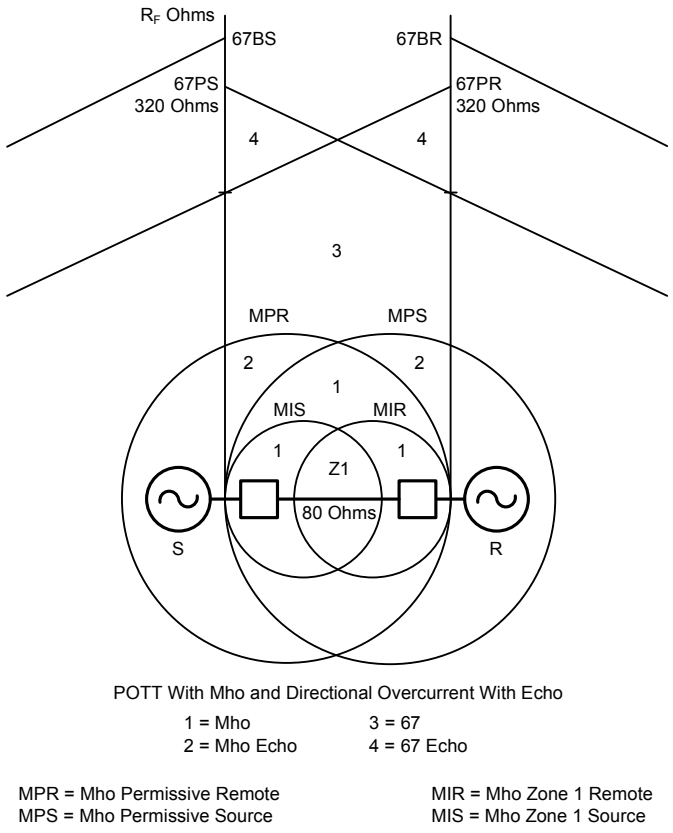

Fig. 7. Long line with strong sources equals little mho expansion

On shorter lines with weaker sources, the element will expand greatly, making it less necessary to use ground directional overcurrent elements (Fig. 8).

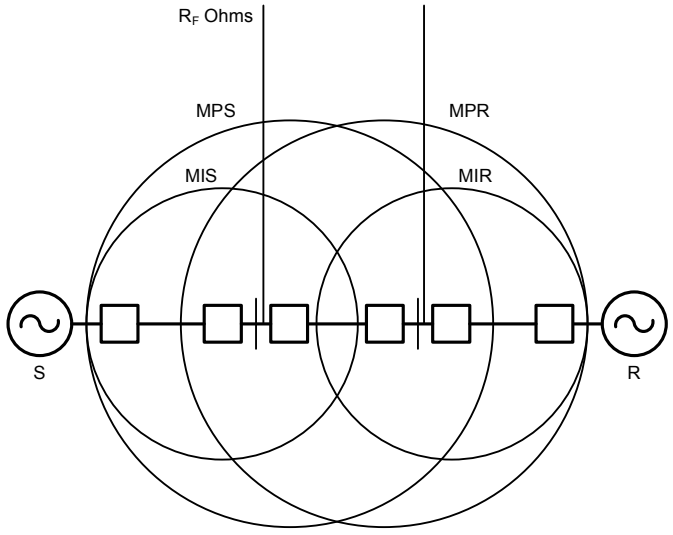

Fig. 8. Short line with weak sources equals great mho expansion; no need for directional overcurrent elements for R_F coverage

The following are some of the conditions that have caused overtrips:

- **Mutual coupling effects**. These effects can cause directional element miscoordination. Using negative-sequence directional elements and negative-sequence overcurrent elements can prevent this type of misoperation.
- **Natural unbalance on the line from inadequate transposition**. There will be some level of standing unbalance on all lines due to imperfect transposition. This unbalance increases and becomes a problem on through faults. In some cases, during low-grade faults, the forward-reaching element sees the fault while the reverse-reaching blocking element at the remote end may not. The additional unbalance created by insufficient line transposition is just enough to cause a directional element miscoordination.
- **Switching transients**. Inrush and power swings from switching operations are sometimes enough to trigger sensitive overcurrent elements. Pole scatter, especially on gang-operated switches, can look like a low-grade fault to a very sensitive ground overcurrent element [1] [2].
- **Testing anomalies and CT (current transformer problems and inaccuracies**. Some utilities have experienced echo trips during testing. CT problems can cause enough unbalance under load to create an apparent fault condition and allow an echo trip. Several of these incidents have occurred in the Northeast in the past several years. An overtrip occurred in Massachusetts on a POTT scheme due to CT error, causing very sensitive directional overcurrent elements to miscoordinate [3]. For more information, see the Appendix of this paper.
- **Nonhomogeneous load unbalance**. This can cause disagreements between forward- and reverse-looking directional overcurrent elements.
- **Other complex low-grade faults**. There are a variety of low-grade faults that could cause race conditions when using very sensitive directional overcurrent elements.

Some possible solutions include the following:

- **Supervise echo back with undervoltage elements**. Simple logic can be added to the POTT echo scheme to require the voltage on one or more phases to drop below nominal in addition to checking that no reverse-looking elements are picked up. This adds more security to the echo logic (Fig. 9).

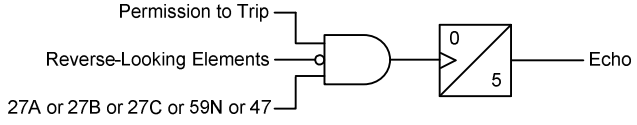

Fig. 9. Adding voltage supervision to echo logic

- **Turn off the echo-back function**. Some utilities have decided to turn off the echo logic [3]. This should be done only after careful study to determine that each terminal will always have an adequate source to pick up a forward-reaching element. The risk is that the line has to clear on backup for some faults.
- **Use echo with mho and quadrilateral elements—no echo with directional overcurrent permissive elements**. As an alternative to turning off the echo-back function, echo logic can be maintained on the more secure mho and quadrilateral permissive elements, and another POTT logic without echo can be built using a second transmit and receive signal. Using a modern digital channel with multiple transmit and receive bits opens up many possibilities, such as the proposed dual POTT scheme shown in Fig. 10.

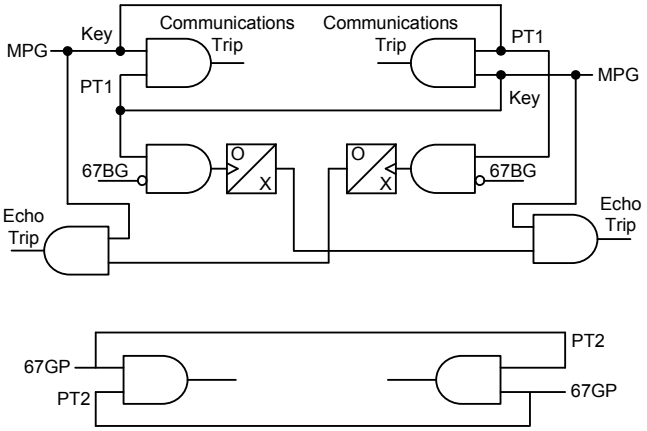

Fig. 10. Dual POTT scheme

- **Use medium time delays on low-set ground directional and negative-sequence directional permissive tripping elements to coordinate with Zone 1 on remote sections**. Add a medium time delay to low-set permissive directional overcurrent elements. A delay of 5 to 7 cycles adds significant security at the cost of a slightly longer overall clearing time for the highest impedance faults only. This scheme will be less dependable than a POTT scheme with instantaneous directional overcurrent elements but more dependable than a POTT scheme with impedance elements only. This POTT scheme with medium delays on the most sensitive elements is the middle ground, perhaps achieving a better balance between dependability and security (Fig. 11).

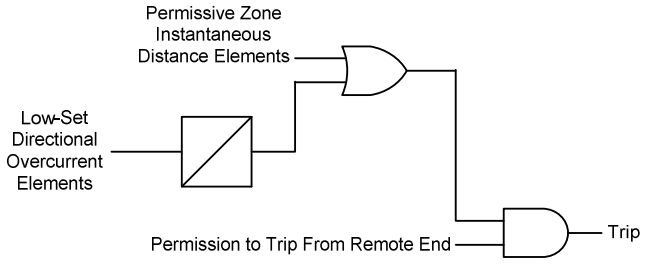

Fig. 11. Adding medium delays to sensitive ground directional overcurrent elements

- **Use asymmetrical directional elements**. Forward and reverse directional elements should never be allowed to race in a POTT scheme with echo. This was the root cause of the misoperation discussed later in the appendix. The remote reverse directional overcurrent element is critical to the security of the scheme. Many relays provide minimum current settings for directional elements in each direction. Reverse settings should always be set more sensitively than the forward settings to provide adequate coordination. For example, the reverse directional element current permissive could be set at the minimum as long as it is not picked up under maximum load, and the forward directional element current permissive is set at three to five times that current. The more asymmetry between the settings, the more secure the coordination. The downside is that minimum forward sensitivity is limited by the forward directional element setting. This is a necessary tradeoff to provide security. Some directional elements also have impedance thresholds that warrant careful study when setting up a POTT scheme with very sensitive directional overcurrent elements. The idea is again to provide more sensitivity in the blocking (reverse) direction than in the tripping (forward) direction. This concept will be discussed later in the directional elements section.

B. Blocking Schemes

1) DCB Schemes

DCB schemes use forward overreaching elements for tripping and reverse elements for blocking. The forward overreaching elements are on a short, typically 0.75-cycle to 2-cycle, time delay. The remote-end reverse-looking element is tasked with sending a block signal to the local forward overreaching element for off-section faults before the time delay expires. Sufficient margin is required to ensure a race condition does not occur. Setting this timer is probably the most important part of this scheme. The relay engineer must consider the relative operate times of the forward- and reverse-looking elements, output contact time, input recognition time, channel time, and processing time or inherent delay in electromechanical relays. Because the DCB scheme depends on the communications channel for blocking rather than tripping, it leans much more toward dependability and much less toward security. Security can be increased by using a reliable communications system, setting the reverse-looking blocking element more sensitively than the forward element, and using a short delay time that is sufficient for all faults plus adequate margin. With these criteria in mind, we will look at the DCB scheme with various relay elements used for tripping and blocking, as well as their sensitivities.

The following are some of the most popular variations of DCB schemes:

- **DCB with mho elements**. This scheme is easy to coordinate with reverse-looking blocking elements and is secure as long as the channel is available (Fig. 12).

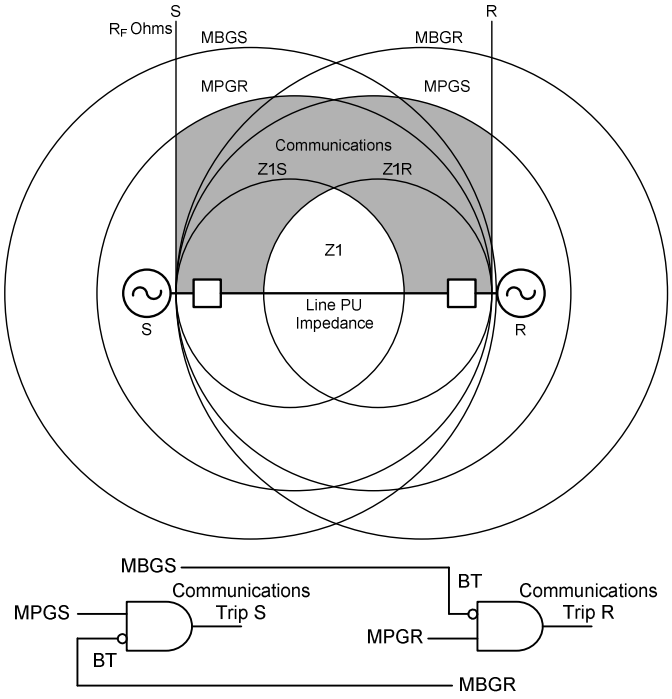

Fig. 12. DCB scheme with mho elements

- **DCB with quadrilateral elements**. DCB with quadrilateral impedance elements provides excellent resistive fault coverage on longer lines with stronger sources where mho elements would not achieve great expansion. This scheme is easy to coordinate with reverse-looking blocking elements and is secure as long as the channel is available (Fig. 13).

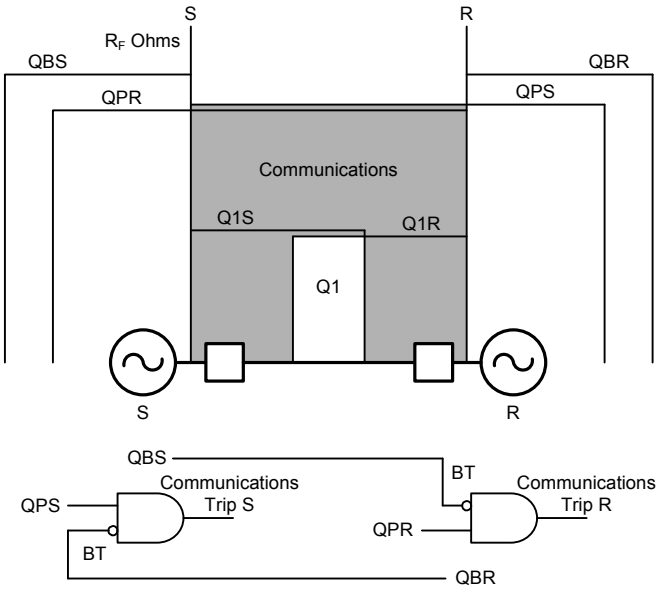

Fig. 13. DCB with quadrilateral elements

- **DCB with directional overcurrent elements**. Setting up a DCB scheme with directional overcurrent elements can be challenging to apply. Adequate study and consideration of the coordination between tripping and blocking elements are necessary. Nondirectional blocking elements may have to be used to coordinate with very low-set forward elements.
- **DCB with nondirectional overcurrent blocking**. Using a nondirectional overcurrent blocking element provides the best security in the DCB scheme at the cost of some additional overall clearing time because the element must drop out before a trip can occur.

DCB improvements include the following:

- **DCB with medium time-delayed directional overcurrent elements**. A DCB scheme with traditional short coordination time-delayed mho or mho and quadrilateral elements combined with medium time-delayed directional overcurrent ground elements can be a very good compromise between dependability for high-impedance faults and overall scheme security (Fig. 14). Slowing down more sensitive elements allows them to coordinate more securely with pilot schemes on neighboring line sections.

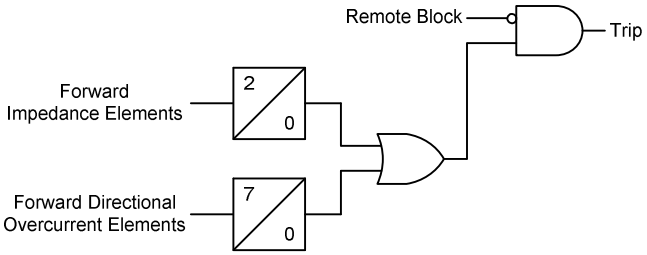

Fig. 14. DCB with medium time-delayed directional ground overcurrent elements

- **DCB with voltage supervised directional overcurrent elements**. As an alternative to or in combination with Fig. 14, supervising directional ground overcurrent elements with voltage elements adds another layer of security for DCB schemes (Fig. 15). Fault studies should be run and the voltage noted for expected high-impedance faults. The voltage supervision setting must be low enough to block conditions that look like faults but are not. The setting should also block off-section faults, which should be modeled in the fault study. The voltage setting must be high enough to allow expected high-impedance faults to be seen by the directional element.

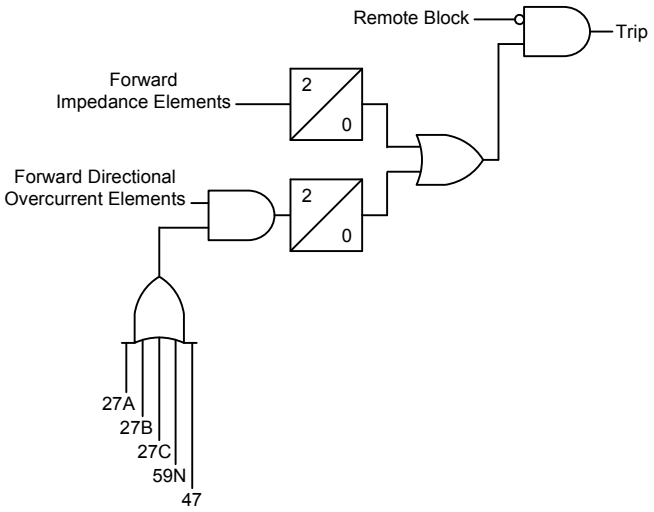

Fig. 15. DCB with voltage supervised directional ground overcurrent elements

- **DCB with asymmetrical directional element settings**. Providing a secure level of asymmetry between forward and reverse directional elements was discussed in the POTT scheme as well. Many relays provide two or more methods of directional control that can be manipulated in logic to ensure reverse-looking directional elements provide more coverage than forward directional elements.

2) DCUB (Directional Comparison Unblocking) Schemes

DCUB uses a communications channel with two frequencies. Normally, the channel transmits a guard signal. When the forward overreaching element picks up, the guard signal drops out, and a permissive trip signal is sent. Permission to trip is allowed for a short duration immediately after the guard signal drops out. This allows tripping in the case of a power line carrier system where the signal is being blocked by the fault. This scheme is considered a blocking scheme but shares very similar logic to the POTT scheme. Additional dependability is gained to allow tripping immediately after fault inception while sacrificing some security because the tripping signal is in doubt. The same recommendations listed to solve problems for POTT schemes are recommended for DCUB schemes as well.

C. Other Impedance and Directional Comparison Schemes

A new hybrid protection scheme is developed in [4] whereby elements of a POTT scheme and DCB scheme are combined. The protection scheme requires the transmission of an overreaching permissive element and a reverse-looking element at the same time in an attempt to combine the best aspects of the POTT and DCB schemes.

As an alternative, relay settings groups could be switched based on system conditions to provide a POTT scheme during periods where security is paramount and a DCB scheme when more dependability is desired. System reconfiguration is another consideration, such as the case of a tapped line that could utilize a DCB scheme but automatically revert to a POTT scheme when the tap is open (Fig. 16). Modern digital communications systems with multiple transmit and receive bits over a reliable digital channel provide a conduit for both schemes.

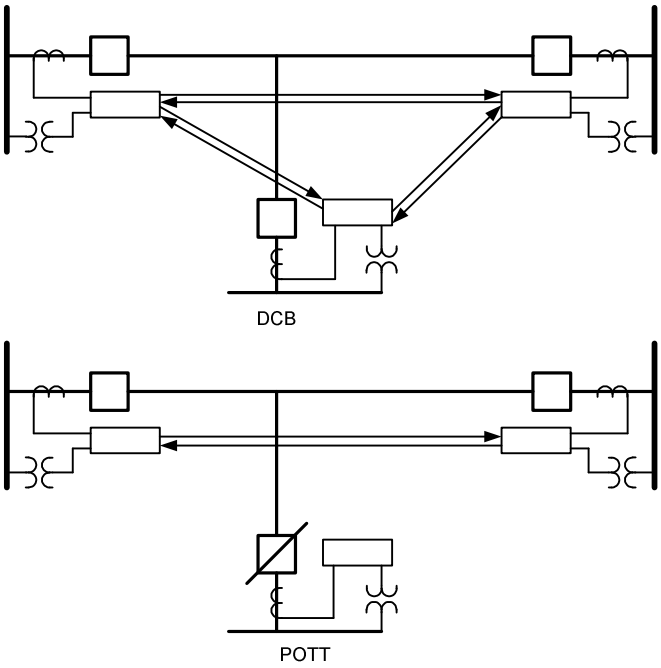

Fig. 16. DCB scheme reverts to POTT scheme when tap is open

D. Line Current Differential Methods

1) Phase Comparison

Phase comparison differential systems have been around for a long time (Fig. 17). A square wave is generated representing current phase and magnitude and then sent to the remote end. A delay is added to the received signal. Then the local and remote square wave signals are added to determine a trip signal. These systems have performed well over the years but can be unpredictable and hard to set.

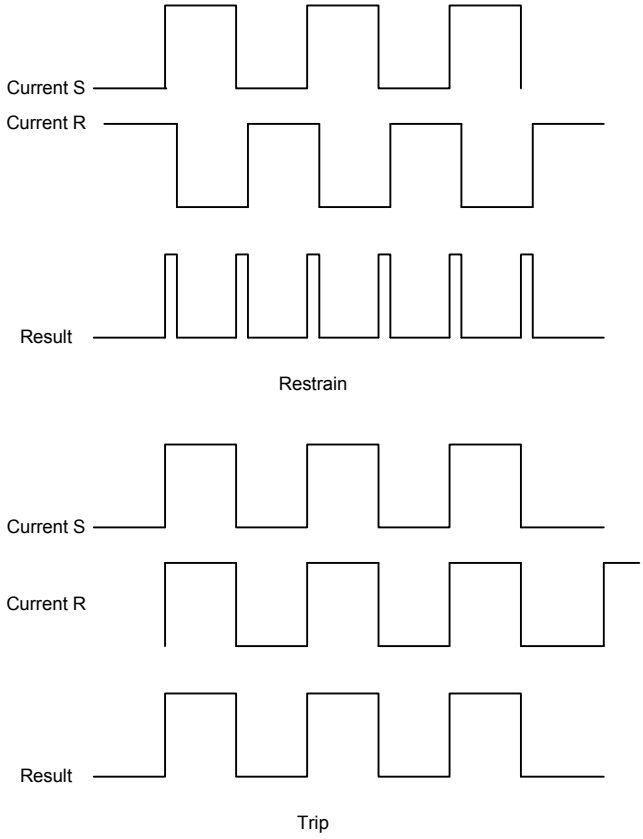

Fig. 17. Phase comparison

2) Percentage Restraint Line Current Differential

Percentage restraint line current differential uses the traditional transformer differential characteristic (Fig. 18) to produce restraint and tripping regions. Challenges to finding the correct slope and breakpoints between slopes will be discussed later in Section II, Subsection A.

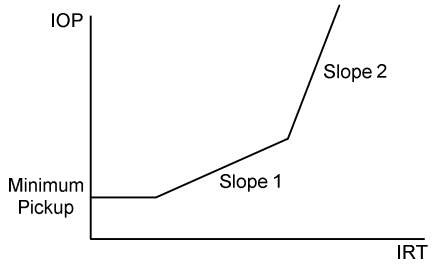

Fig. 18. Traditional dual-slope percentage restraint

3) Alpha Plane Current Differential

Alpha Plane current differential uses a digital channel to send complete current analog information to the remote end, where the quantities are used to calculate phase-, negative-, and zero-sequence quantities for use in a unique differential element operating in the Alpha Plane (Fig. 19). This Alpha Plane characteristic provides an excellent determination of fault magnitude and phase angle. The characteristic provides excellent security for CT saturation, communications delays, and line-charging current.

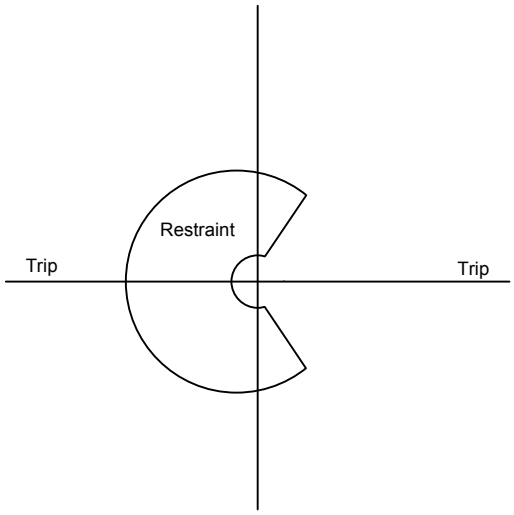

Fig. 19. Alpha Plane differential

E. Other Transmission Line Protection Considerations

1) Directional Elements

Directional elements are a big consideration in how sensitive a relay scheme can be set [2], but the practical limits required for a secure tripping scheme often require settings above the minimum sensitivity. As discussed earlier in the paper, directional elements are extremely critical in the application of protection schemes because they directionalize very sensitive overcurrent elements. We want to pick a directional element design that provides as much sensitivity as possible while remaining very secure. Settable impedance directional elements are the way to achieve this. They allow the user to customize the directional element for the line being protected. Relative strength of sources (Thévenin equivalent) in front of the relay and behind the relay can be very useful information for the directional element, allowing it to gain intelligence about the system. Fig. 20 shows graphically how the directional element offsets in the proper tripping direction based upon the impedance settings entered. The directional element rejects incorrect current and voltage signals that could be presented to the relay in the form of CT errors and capacitor coupling voltage transformer (CCVT) errors and transients.

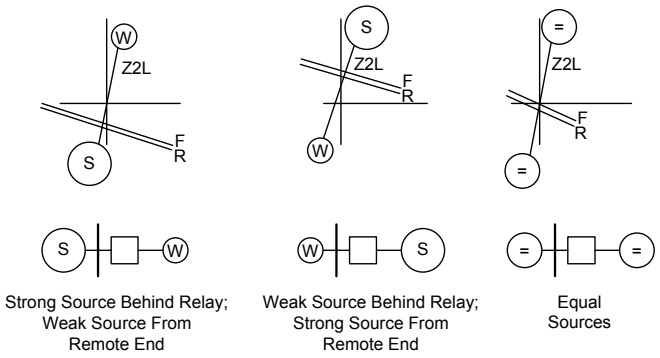

Fig. 20. Directional element offset based on fault duty

Another very important feature of a directional element that is secure while maintaining adequate sensitivity for low-grade faults is the ability to maintain maximum sensitivity based on loading and fault conditions. As discussed earlier in the paper, CT errors, CCVT errors and transients, transposition errors, switching transients, and other conditions can cause false directional element assertions. A secure and dependable directional element design allows the user to set a ratio of unbalanced to balanced current for element torque control based upon the expected errors and operating conditions for that system (Fig. 21).

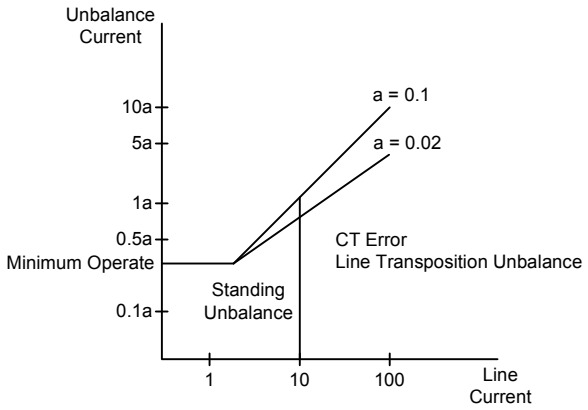

Fig. 21. Directional element desensitizes as current increases

Microprocessor-based relays include smart directional systems that can select the appropriate directional element by looking at input quantities that will be dependent on system conditions. At the inception of the fault, the relay selects the best method of determining direction from the negative-sequence, zero-sequence, and current-only directional methods. Using this system ensures directionality will be available so that backup nondirectional overcurrent elements will not produce an overtrip.

2) Relative Speeds of Various Protection Elements

The relative speeds of various protection elements must be considered when putting together a protection scheme. Nondirectional overcurrent elements are the simplest and fastest elements. Directional elements are next in line in complexity and operating speed. Finally, impedance elements are the most processing intensive and require just a little more time to operate. Distance elements operate much faster when well within the set reach and progressively slower when at the threshold of the reach. Operating speeds of various types of output contacts and relay inputs must also be considered when designing a protection scheme.

3) Three-Terminal Line Considerations

Normally, three-terminal lines have at least one weak-feed terminal. Two weak-feed terminals complicate logic in POTT schemes.

Infeed conditions cause the impedance measured at a terminal to change. These apparent impedances can become quite high. Fault studies must be run to determine which relay elements provide the best coverage under various conditions and faults.

Outfeed conditions are possible when there is a large disparity in the strength of the sources. A fault on the line could be fed by a strong terminal, backwards through the weakest terminal, with the current returning through the third terminal in the forward direction. The outfeed terminal will improperly send a block signal.

4) Synchrophasor-Based Protection

As we progress further into the twenty-first century, communications systems continue to proliferate, allowing more sophisticated, data-intensive protection methods to be utilized. Synchrophasors incorporated into protective relay firmware have already proven to be an invaluable tool for testing and predicting system stability by measuring it in real time [5]. This proves to be the most powerful means of effecting system-wide and nationwide electric grid security.

II. Differential Protection

A. Bus Differential

Bus differential protection is even more critical to nation-wide grid security than line protection in most instances. Loss of a single bus includes several lines and has a huge impact on the system. Fault currents are very high at buses, creating major complexity when considering protection. CTs are pushed to their limits, resulting in saturation or at least some nonlinear performance.

Dependable bus protection must have very good sensitivity to see all faults on the bus and provide a subcycle trip. Secure bus protection restrains for all through faults and tolerates some CT saturation. Traditionally, low-impedance percentage restraint bus differential relays have one or two slopes the user must set.

The slope settings should be low or sensitive enough to see all faults, including potential high-impedance faults, but must be high or desensitized enough to restrain for all potential through faults. Very high through faults cause some amount of CT saturation that must be estimated when considering the slope setting. If the system gets stronger over time, fault currents increase, causing additional CT nonlinearity. If the breakpoint between the first slope setting and the second slope setting is too high, a misoperation could result. The relay engineer is presented with a quandary: err on the side of dependability or security? In recent years, newer low-impedance bus differential designs have emerged that make

the protection engineer's job easier. These relays sense whether a fault is internal or external at fault inception and adjust the slope dynamically (Fig. 22). This intelligent differential relaying method preserves sensitivity and dependability while maintaining excellent security.

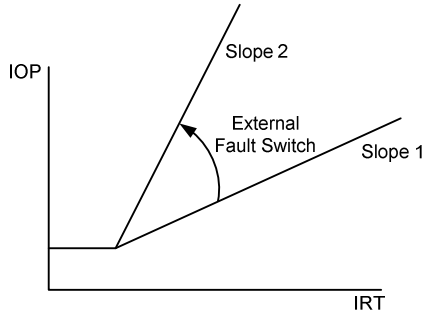

Fig. 22. Smart dynamic percentage restraint

B. Transformer Differential

Transformer differential protection is evolving to keep pace with evolving transformer designs. Modern designs have more efficiently designed cores, as well as more and better quality material in the core. New technology and modern requirements for noise reduction are two of the driving forces.

Dependable transformer protection must have very good sensitivity to see all faults in the transformer, such as low-grade faults close to the neutral connection, and provide a subcycle trip to limit damage. Secure transformer protection restrains for all through faults and tolerates some CT saturation. In addition, secure protection restrains during transformer energization every time.

Newer bus differential designs mentioned in the previous section make use of dynamic slopes to increase both dependability and security at the same time. These designs are also incorporated in transformer differential relays [6].

Newer transformer relay designs also use new methods for detecting transformer inrush. Harmonic restraint can be a better solution in many cases, desensitizing the percentage restraint unit just enough to prevent false tripping rather than blocking it entirely (Fig. 23).

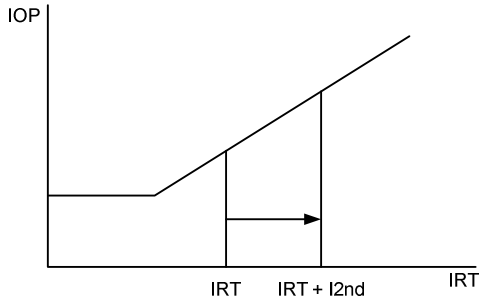

Fig. 23. Harmonic restraint

III. Distribution Protection

Protection of distribution systems ranges from the very simple to the very complex because of the diversity found in these systems. Loads range from simple, single-phase residential to complex networks of looped feeders found in major industrial complexes and hospitals. Distribution protection thus requires as much or more study and consideration as goes into EHV (extra-high-voltage) protection. Some considerations in distribution protection include:

- **More exposure**. Distribution feeders can be quite large, considering the number of taps and laterals. Many feeders are surrounded by trees and have limbs in very close proximity. Exposure to road hazards, train and water crossings, and various other terrain is of particular concern.
- **Safety issues and downed conductors**. The general public come much closer to distribution feeders and equipment than to transmission systems, so safety hazards are a bigger concern. Arc-flash and electrocution hazards are ever present.
- **Mixed load profiles**. Loading profiles on a mixed-use feeder are extremely hard to predict. We may not know what the maximum loading will be on some feeders.
- **Much standing unbalance that is constantly changing**. Balancing feeders can be an effort in futility. The amount of standing unbalance on a feeder varies minute to minute and continually evolves month to month and year to year.
- **Unknown loads and generation**. Many large-energy consumers, such as air conditioners, spas, pools, and pond pumps, are continually being added to the system. Emergency generators and cogenerators are also being added daily, complicating protection.
- **Many levels of coordination**. As reclosers become more economical, there will be more levels of coordination to contend with, especially on large, important feeders.
- **Many different and unknown transformer connections**. Delta-wye transformer connections provide ground sources, and other connections cause ferroresonant conditions on feeders, adding unknowns and complications for protection engineers.
- **Fuse-saving versus fuse-forcing philosophy**. The goal is to maintain a continuous supply of power to customers of all types. A balance must be achieved to provide uninterrupted service to as many customers as possible, while sacrificing as few as possible. Under normal operating conditions, this means forcing a fuse

feeding a single customer or a small section of customers to operate instead of operating a recloser or feeder circuit breaker at the substation. Line crews can be dispatched in a reasonable amount of time to troubleshoot, replace the fuse, and restore service (Fig. 24).

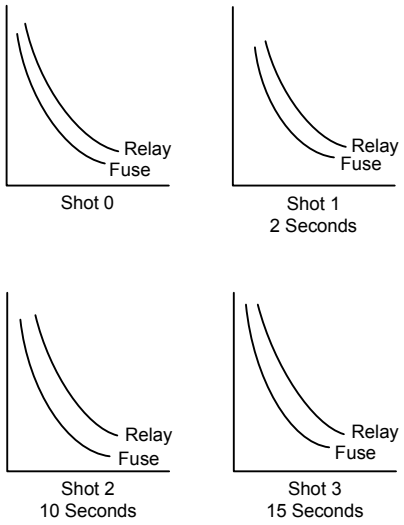

Fig. 24. Fuse-forcing scheme (three reclosers)

During storm conditions, line crews are stretched thin and will not be able to provide fuse replacement in a reasonable amount of time. A fuse-saving setting scheme could be implemented to save valuable crew time and minimize customer outage time. The recloser and substation protection adds sensitive instantaneous elements to beat the minimum melt time of the fuse. Temporary faults clear during the reclose intervals. More reclose intervals can be added, with instantaneous elements enabled right up until the last reclose, when the fuse must finally be forced (Fig. 25).

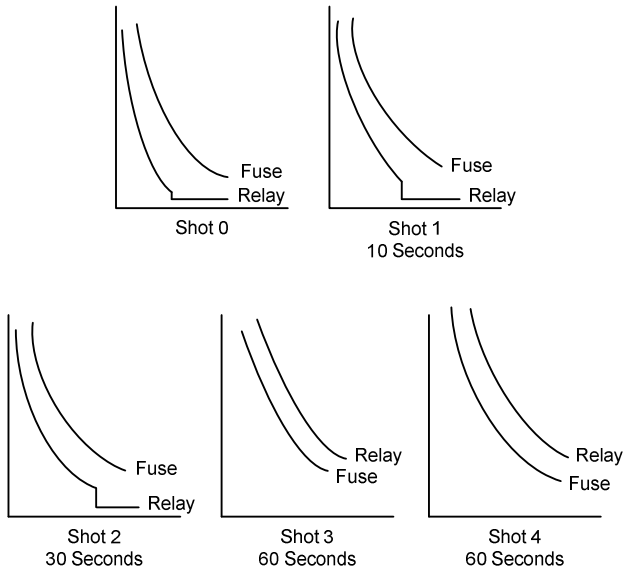

Fig. 25. Fuse-saving scheme (four reclosers)

Microprocessor-based relays with multiple settings groups can easily be switched by SCADA (supervisory control and data acquisition), simple phone line connections, or even local weather stations. Use of modern technology to change an operating philosophy in real time provides the best balance between dependability and security, depending on system conditions.

Automatic distribution system reconfiguration has become possible using the ample logic available in microprocessor-based relays. Using communications between relays, these reconfiguration schemes perform quite well. As mentioned previously, efficient transfer schemes provide the least level of voltage disturbance to the least number of customers for the least amount of time.

Open transition transfer schemes detect and clear the faulted section and then close the normally open breaker to pick up the nonfaulted sections from another source (Fig. 26). Normally, an open transition transfer is desired rather than a closed transition, or fast transfer, to avoid voltage disruption when the new source is a different transformer.

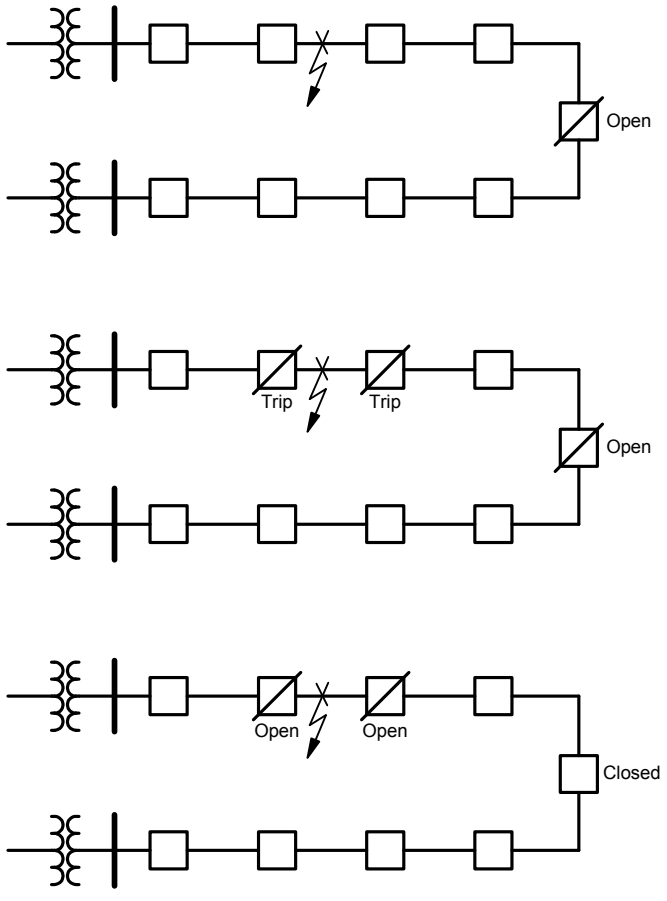

Fig. 26. Open transition transfer

Closed transition transfer schemes can be utilized as a compromise to operating in a continuous looped mode (Fig. 27). Normally, both sources are from the same transformer, so there is little risk of further disruption of the voltage profile when paralleling into the faulted section.

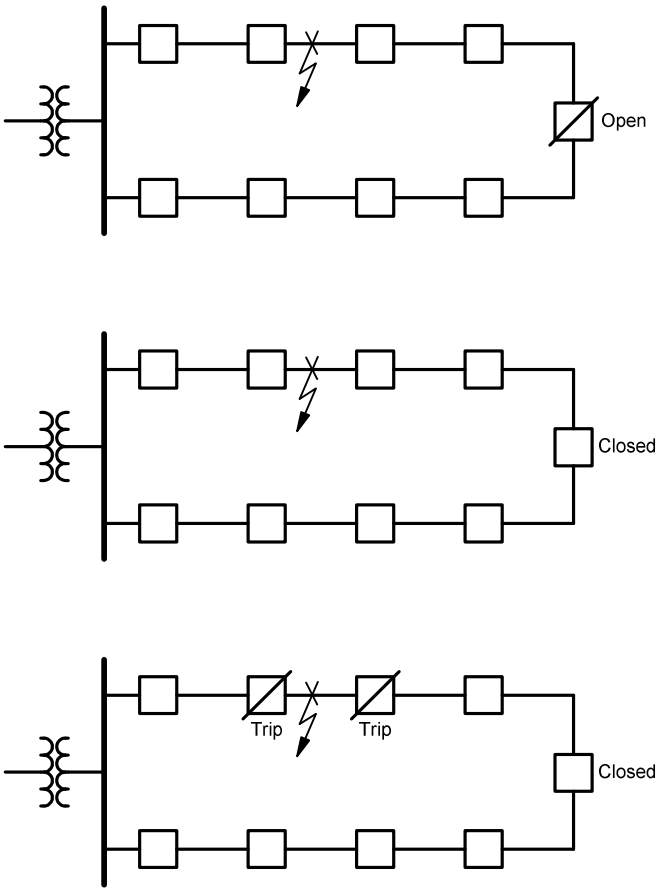

Fig. 27. Closed transition transfer

Looped feeders serve loads from two sources (Fig. 28). Directional elements and communications schemes discussed earlier in this paper can be utilized to provide very reliable service to distribution customers. Many microprocessor-based distribution relays provide built-in POTT, DCB, and DCUB schemes. As discussed before, relay logic can be used to build any protection scheme the user can dream up.

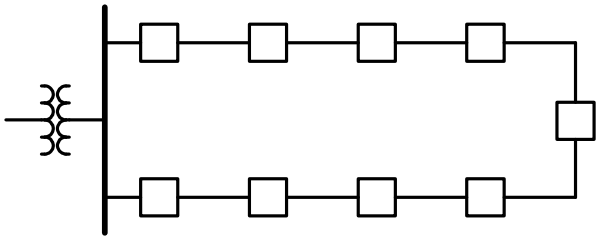

Fig. 28. Looped feeder

Communication is critical to increasing distribution system performance. Costs for fiber and radio have dropped drastically over the last ten years. Now is an excellent time to utilize communications technology to make the grid smarter, and as a result more reliable, by finding the balance between dependability and security.

IV. Conclusion

Walking the line between dependability and security requires continual data gathering and study of installed protection systems. Advanced relay protection systems allow protection customization to a level that was never possible before. Communications systems continue to rapidly improve and proliferate. New relay algorithms that provide smarter protection have been developed. The protection engineer should consider the following when installing new relaying or reviewing existing relaying schemes:

- Take advantage of relay logic to customize standard schemes to make them more dependable and secure.
- Supervise or delay very sensitive relay elements to gain security.
- Utilize dynamic slope on bus and transformer differential applications to gain dependability and security at the same time.
- Install and utilize communications on important distribution loops. Utilize relay logic to provide automatic reconfiguration.
- Study standard settings to verify their applicability before applying.
- Install digital communications on transmission systems to get multiple transmit and receive bits. More advanced schemes can be implemented for smart grid applications when relays can intelligently communicate.

V. Appendix

On January 11, 2008, the National Grid Control Center reported that at 13:32:03, a lightning strike caused a fault on the 115 kV E157 line between the Millbury and Northborough Road terminals. Simultaneously, the 345 kV 313 line operated at the Millbury terminal only. The control center reported that the 115 kV E157 line tripped and autoreclosed correctly at both terminals, and the Millbury terminal of the 313 line operated simultaneously to the E157 line fault and autoreclosed.

Comparing the relay fault records for the 313 POTT relay at Millbury and Wachusett and the associated relay settings, someone noticed that at the trigger point, the magnitude of the reverse-looking ground overcurrent blocking element at Wachusett was higher than the preset pickup level. However, it did not pick up because the reverse-looking directional element did not assert. As a result, the reverse-looking ground overcurrent blocking element failed to block the echo of the received permissive trip signal at Wachusett, and it echoed back to Millbury. Based on the records captured by the relays, the 3I2 (negative-sequence current) sensed by the reverse directional element at Wachusett was on the edge of asserting but deasserted, even though it had been set at the minimum tap to provide maximum sensitivity. The 3I2 sensed by the forward directional element at Millbury was just above pickup.

In order to improve the security of the POTT scheme and prevent any parallel line fault from causing an operation on the POTT scheme for external faults, the echo logic application for the 313 line was disabled. A review of other lines in the area resulted in the disabling of the echo logic in POTT schemes on an additional seven transmission lines.

As a result of the investigation, a recommendation to reevaluate the use of the echo applications in POTT schemes was made. The determination was that there are cases where the echo feature could provide needed protection system dependability; however, the use of echo logic in POTT schemes should be evaluated carefully for each transmission line application because an improper application affects protection system security.

For more information on this investigation, see [3].

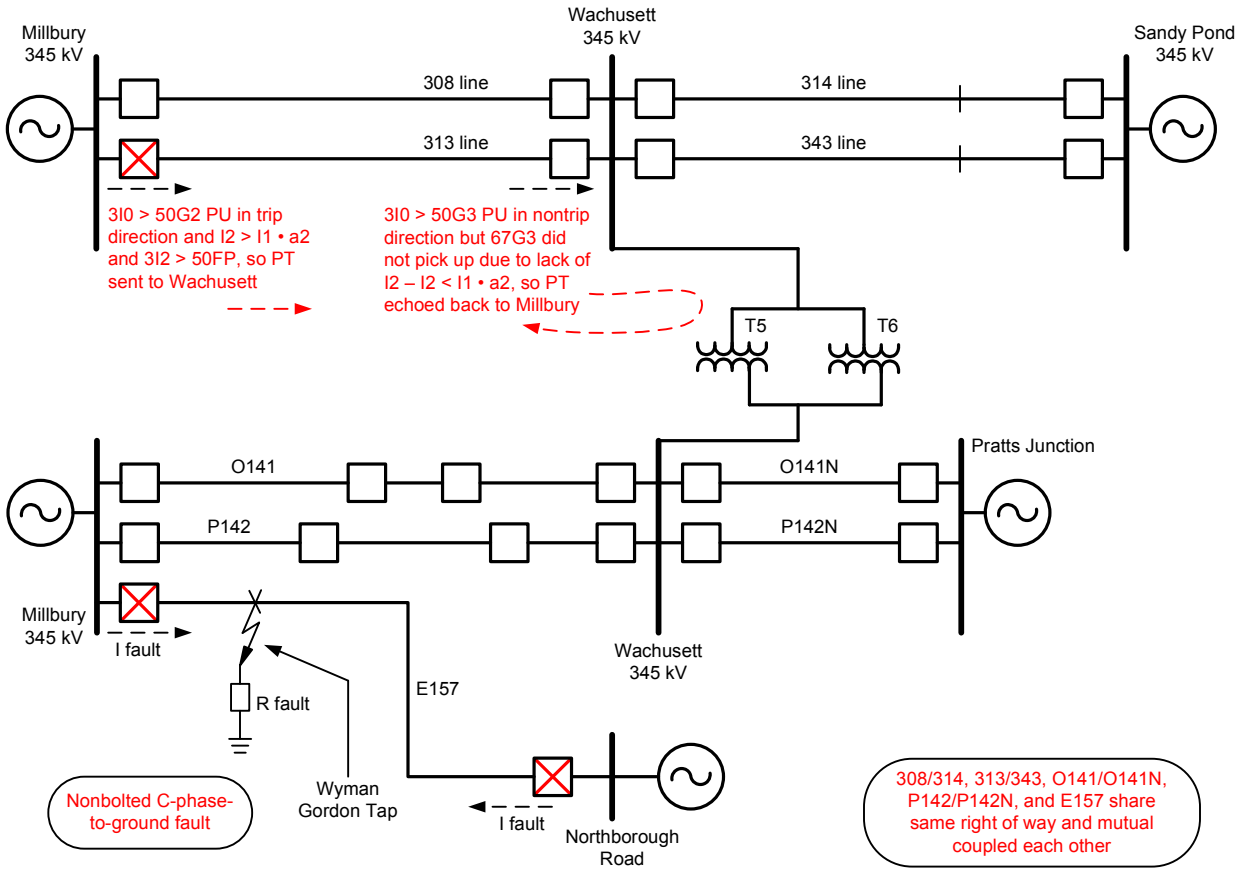

Fig. 29. E157 fault with response of 313 echo logic at Wachusett

VI. References

[1] J. Mooney and J. Peer, "Application Guidelines for Ground Fault Protection," proceedings of the 24th Annual Western Protective Relay Conference, Spokane, WA, October 1997.

[2] J. Roberts, E. O. Schweitzer, III, R. Arora, and E. Poggi, "Limits to the Sensitivity of Ground Directional and Distance Protection," proceedings of the 1997 Spring Meeting of the Pennsylvania Electric Association Relay Committee, Allentown, PA, May 1997.

[3] Y. Lu and J. Pond, "Analysis of POTT Scheme Operation for an External Fault," proceedings of the 12th Annual Georgia Tech Fault and Disturbance Analysis Conference, Atlanta, GA, April 2009.

[4] E. O. Schweitzer, III and J. J. Kumm, "Statistical Comparison and Evaluation of Pilot Protection Schemes," proceedings of the 24th Annual Western Protective Relay Conference, Spokane, WA, October 1997.

[5] C. Araujo, F. Horvath, and J. Mack, "A Comparison of Line Relay System Testing Methods," proceedings of the 33rd Annual Western Protective Relay Conference, Spokane, WA, October 2006.

[6] A. Guzmán, N. Fischer, C. Labuschagne, "Improvements in Transformer Protection and Control," proceedings of the 62nd Annual Conference for Protective Relay Engineers, College Station, TX, March 2009.

VII. Biographies

Jeffrey M. Pond has been an employee of National Grid for 28 years. He is a senior engineer in the protection standards and support department, where he is responsible for the analysis of transmission and distribution system disturbances. He is also responsible for the selection, configuration, and maintenance of disturbance recording equipment. Previously, Jeff worked for the substation integration team and the relay and telecommunications operations group. He received an associate's degree in electrical engineering technology from Wentworth Institute of Technology in Boston, MA, a BS in business management from Lesley University in Cambridge, MA, and an MS in power systems management from Worcester Polytechnic Institute in Worcester, MA. Jeff is a member of IEEE and is active in several working groups of the Power System Relaying Committee.

Yujie Irene Lu has been employed with National Grid since 1990. She is a principal engineer in the department of protection engineering, where she performs system analysis for short-circuit conditions, designs protection systems on a conceptual basis, specifies equipment, and determines relay settings. Since 2004, Irene has been working as a lead protection engineer on the installation of two major 345/115 kV GIS transmission substations for National Grid in the New England area. In addition, she analyzes disturbances on transmission and supply networks. Previously, she worked for the Department of Energy of China for 5 years. Irene received a BSEE degree in power systems engineering from Huazhong University of Science & Technology in China and an MSEE from Virginia Polytechnic Institute in Blacksburg, VA. She is a member of IEEE and a registered professional engineer in MA.

James E. Mack has a BSEE degree from Louisiana State University in Baton Rouge, LA. He has held various positions in his 29 years in the electric utility industry and has experience with transmission, distribution, and SCADA systems and nuclear power plant construction. Jim joined Schweitzer Engineering Laboratories, Inc. (SEL) in 1996 as a field application engineer, where he assists customers in the application of SEL relays and integration systems.