

# Performance Issues With Directional Comparison Blocking Schemes

Ian Stevens, *Powerlink, Queensland, Australia*  
Normann Fischer and Bogdan Kasztenny, *Schweitzer Engineering Laboratories, Inc.*

**Abstract**—Distance and directional overcurrent protection can provide 100 percent coverage of transmission or subtransmission feeders through the use of teleprotection (communications-assisted tripping) schemes. We briefly review in this paper various types of teleprotection schemes and then present principles to successfully apply a directional comparison blocking scheme (DCB). We amplify these principles by examining the reasons why incorrect tripping occurred on feeders using DCB schemes in five field cases.

Further, we alert readers to the conundrum of using DCB schemes in emerging electricity markets—dependability of protection versus less security of supply. We propose that protection engineers can apply the advantages of digital communications systems, functionality of numerical relays, and increased electricity network infrastructure to intelligently design line protection systems with high dependability and high security.

## I. NOMENCLATURE

Table I contains definitions for abbreviations this paper uses.

TABLE I  
TECHNICAL DEFINITIONS

Abbreviation	Definition
AER	Australian electricity regulator
Blocking Element	Reverse-looking element or element collection overreaching all tripping elements from remote terminal end(s)
DCB	Directional comparison blocking scheme
DEF	Directional earth fault
DOC	Directional overcurrent
End zone	Assuming Zone 1 was set at 80% of feeder length, the last 20% of each end of the feeder
Local relay	Relay closest to the fault
Main 1 or 2	Duplicate protection schemes
NER	National electricity regulator
OPGW	Optical power ground wire
PLC	Power line carrier
POTT	Permissive overreaching transfer trip scheme
PUTT	Permissive underreaching transfer trip scheme
Remote relay	Relay located at remote end of local relay's feeder
SPAR	Single-pole auto-reclose
Teleprotection Scheme	Communications-assisted protection scheme
Tripping Element	Overreaching, forward-looking element or collection of elements that pick up for all intended feeder faults

## II. INTRODUCTION

Transmission and subtransmission feeders usually employ duplicate high-speed protection, such as distance or current differential. A teleprotection scheme enables distance or directional overcurrent protection to provide 100 percent feeder coverage with total fault clearance times of less than about 6 cycles. In recent years, two trends affect line protection.

First, economic and regulatory conditions created by the competitive electricity market environment put renewed emphasis on security of protection. Unwarranted tripping of feeders can cause production and financial losses to electricity customers and electricity market participants. This is particularly true in cases when distributed generation does not enjoy multiple transmission paths, its availability depends on the state of one or just a few lines, or in sparsely populated areas with only a few transmission paths to feed the loads.

Second, means of communication for protection purposes have advanced considerably and have migrated into all-digital systems with built-in redundancy and self-monitoring. However, basic line protection principles did not accompany these advancements to take advantage of the new channel characteristics. Instead, there has been continued replication of solutions originally developed for power line carrier schemes.

For less experienced engineers, we provide valuable insights into the principles of teleprotection, DCB, the effects of load growth, market demands and the beneficial application of digital technology. These factors will challenge engineers' future selections and applications of protection systems and refine the art of line protection.

A transmission utility investigated the performance of a DCB scheme after a series of incorrect trips of healthy feeders that contributed fault current to an adjacent fault. The field cases we present demonstrate the following:

- Effects of the above factors and similar impacts upon a POTT scheme.
- How the key principles could be better achieved when designing and setting schemes.
- Need for protection engineers to understand the impacts of load growth and differing relays.
- Impacts of new technologies upon protection performance and how to fully utilize the disturbance and event recording capabilities of numerical relays.
- Need for effective testing practices that cover unique fault characteristics, interaction of supervision and

distance elements in numerical relays, and the use of COMTRADE testing files.

- Need to review and understand exact operating principles of the coordinated functions, particularly if a scheme uses varying models of relays or those from various manufacturers.

As a consequence, the prudent engineering response was to reconsider the selection of protection systems because of the following:

- Rules (AER) and requirements of the electricity market and the actions of its regulator, principally to encourage economic increase in security of supply;
- Advantages of digital communications technology to provide robust signaling and redundancy;
- Expanding communications infrastructure in a growing power systems network;
- Increased functionality of numerical relays such as backup protection, flexible and adaptive logic, secure inter-relay communication and event recording;
- Limitations of distance functions with respect to load transfer capability.

We present these considerations to solicit feedback from protection engineers, with a view toward shaping future protection policy and application.

### III. TELEPROTECTION SCHEMES

The appendices provide more details of distance protection and teleprotection. The following provides the salient points for consideration in this paper.

Duplicate protection systems on transmission feeders provide rapid detection, identification, and tripping (single or three-pole) for all faults occurring within the feeder. Examples of protection systems are current differential, distance, DOC, and DEF. The protective scheme must remain secure (refrain from tripping for all external faults). Electricity rules (NER) may specify fault clearance times for the operation of the electricity market [1].

For distance protection, we can achieve fast tripping for respective Zone 1s of the feeder. We can use teleprotection to trip the remaining end zone(s) in slightly more time (typically an extra 30–50 ms). Typically, this satisfies the performance criteria for network operation, minimizing damage and enabling public safety criteria (see Appendix 1: Types of Teleprotection Schemes). Thus, teleprotection creates a pseudo unit protection of the feeder, although we realize that in practice similar to unit protection it may fail under certain adverse power system and protection system conditions.

We focus in this paper on the DCB scheme, for which key factors for successful application include the following.

#### A. Principal Advantages

Listed below are some of the major advantages a DCB scheme over a permissive scheme.

- DCB is not based on a permissive logic, so there is no waiting for the permissive signal. DCB achieves consistent tripping and speed for the faulted feeder;
- The blocking signal is sent over the unfaulted feeder (e.g., PLC or OPGW);

- Various measures can be taken to improve the security of this tripping-biased scheme;
- Two blocking signals are sent by redundant paths to the remote relay, and either will block the relay when necessary. One path can serve as a duplicate communications system for protection;
- The GUARD signal monitors the health of each communications system. The signal must declare the channel healthy before DCB can operate;
- The blocking signal is generated with low security (sensitive settings) and sent quickly (without security delay) because it does not initiate tripping;
- The protection signaling units, dc supply for blocking signal, and GUARD are monitored. Alarms assert upon a failure.

#### B. Blocking Operation

The operating criteria of the distance and supervision elements are coordinated. The blocking element of the local relay is set to operate for any external fault that the remote relay's tripping element can detect. For the reverse-looking zone, this requires lower pickup values for all critical supervision functions and overlapping of overreaching element distance characteristics at the local relaying point (at line angle and credible arcing faults). Two relays operating with similar algorithms provide the best method for achieving this.

The operating speeds of the distance relays are coordinated over the range of source impedance and fault position for any visible external fault that the tripping element detects. Unfavorable differences (tripping element faster than the blocking element) can be accommodated in the coordination time-delay setting in each relay.

The blocking time delay in each relay accommodates the signal propagation delay in the communications system and a safety margin to ensure correct operation.

The local relay must send blocking signals for any external feeder fault that the remote relay tripping zone can detect. One signal must arrive within the coordinated time delay (blocking time) of the remote relay and block tripping. Note that we must take into consideration the debounce time of the receiving relay input contact when we use physical input contacts to interface the blocking signal.

#### C. Tripping Operation

The operating criteria and speed of the distance and supervision elements do not require coordination. We generally use standard setting criteria for Zone 1; Zone 2 is optimized for fault coverage, so the remote relay Zone 3 coverage is manageable.

The local relay must not send blocking signals for any internal feeder fault. The most arduous case is a near zero voltage fault at the relaying point. The choice of distance relay and its polarizing voltage must ensure directional integrity of Zones 1 and 3. A short lasting blip in the blocking signal, such as might result from transients, is acceptable because it may

cause a slightly delayed operation (not a failure to trip) if it occurs when the coordination timer expires.

#### IV. SAMPLE FIELD CASES

##### A. Introduction

This section describes the performance of DCB schemes based upon the experiences of a transmission utility. Generally, the DCB scheme performances for internal faults were very good. Blocking performances for external faults,

however, were inferior. This is critical for parallel feeders with DCB protection; a fault on one feeder requires the correct operation of the healthy feeder's protection, or else loss of supply will occur.

It is worthwhile to review technology characteristics such as those in Table II for distance relays (see Appendix 5: Distance Relay Technology Characteristics for more detail).

TABLE II  
OPERATING TIMES OF DISTANCE ELEMENTS FOR VARIOUS TYPES OF DISTANCE RELAYS

	Distance Characteristic	Operating Speed 0–60% Reach	Operating Speed 61–100% Reach	Directional Sensitivity	Close-in Fault Selection	Special Features
<b>Analog relay—full scheme</b>	Ordered as mho or quadrilateral	25–35 ms	≤ 45 ms	Acceptable	Acceptable	Purchase Z3 elements
<b>Analog relay—switched scheme</b>		30–50 ms	≤ 65 ms	Acceptable	Special measures applied	Composite element (e.g., voltage-modified overcurrent)
<b>Solid-state relay</b>	Transition–manufacturer dependent	25–35 ms	≤ 45 ms	Better	Good	
<b>Numerical relay (conventional algorithms)</b>	Selectable: mho, quadrilateral, or polygon	20–30 ms	≤ 35 ms	Best	Good	
<b>Numerical relay (high-speed algorithms)</b>		15–30 ms	≤ 35 ms	Best	Good	High-speed algorithm may be selectively applied

**Note:** Operating times in the table are for a 50 Hz system.

For external faults, there are a number of reasons why a DCB scheme must not operate for a healthy feeder that contributes fault current:

- Both relays will see the same current (ignoring the line charging current).
- The local relay will see a different voltage (e.g., smaller, different sequence component values) than the remote relay.
- The external zone fault will consist of healthy feeder current plus infeed current from other sources connected to the substation bus. This infeed magnifies the fault impedance both relays detect and does not erode their coordination. However, upon scheme misoperation, any fault location the scheme identified on the healthy feeder relay will be incorrect, thus clouding the post-mortem analysis.

All records we present in this paper are for a 50 Hz system.

##### B. DCB Undesired Operation Events

###### 1) Uncoordinated Sensitivities

As Fig. 1 shows, we used DCB schemes for two parallel feeders. Bird excrement caused an earth fault on Feeder 1 when the insulator flashed over. The DCB scheme correctly tripped Feeder 2 (F2) (see Fig. 3), but the healthy Feeder 1 (F1) also tripped because there was no blocking signal. Subsequent standard testing of this protection found no

problems. The investigation revealed these interesting causes for misoperation:

- Analysis of fault current contribution on F1 revealed low values of zero-sequence current ( $I_0$ ) (see Fig. 4). This phenomenon resulted from the location of the fault close to a substation with four transformers (earthed neutral points of wye windings). These transformers provided a low, zero-sequence impedance that effectively short circuited the zero-sequence impedance of the healthy feeder. Therefore, only a small amount of zero-sequence current flowed in F1. In retrospect, this unique current composition explains why the standard tests only proved that the relays operated correctly with test currents of equal sequence currents.
- Fig. 5 shows that as the number of transformers decreases, the proportion of  $I_0$  in F1 increases until it returns to normal with no transformers in service.
- Fig. 6 shows that as the fault location (in the faulted feeder) moves farther from the substation, the proportion of  $I_0$  in healthy F1 increases.
- The reasons for this phenomenon are evident in Fig. 2, which shows the zero-sequence network for this fault:
  - The three autotransformers and the star/delta transformer (all star points are directly earthed) effectively shunt the F1 impedance. Therefore the

majority of  $I_0$  flows in these transformers. The circuit breakers (shown as squares in Fig. 2) help illustrate the impact of transformers being removed from the network: more  $I_0$  flows in F2, in accordance with Fig. 6;

- The star/delta transformer's zero sequence impedance,  $Z_0$  is significantly less than the  $Z_0$  for an autotransformer. Fig. 5 shows this clearly in the ranking along the ordinate axis;
- As the fault location (in faulted feeder) moves farther from the local substation, the remnant faulted feeder's impedance increases. Therefore, the magnitude of  $I_0$  flowing into the fault from the local substation (Local Sub) decreases. In relative terms, therefore, the proportion of  $I_0$  in healthy feeder, F1, increases.
- An examination of the sequence current composition for the faulted feeder (adjacent to the transformers) showed that it remained nearly equal (see Fig. 3 and Fig. 7). This means that the fault record data file from the tripping relay cannot be used to test the block sending relay.
- The Zone 3 reach of the local relay was correct, and the Zone 2 reach for the remote relay was correct. However, the overcurrent supervision elements for each relay were set differently, with the remote relay having approximately three times more sensitivity. This resulted in a gap between the tripping Zone 2 coverage and the blocking Zone 3 coverage for external ground faults.

Effectively, the Zone 3 element saw the fault, but the supervision element stopped the blocking signal from being sent because the  $I_0$  value was less than the set threshold. Subsequently, the relay manufacturer disclosed that the value of  $I_0$  also had to exceed the negative-sequence settings in the supervision element before the faulted phase selection algorithm would initiate. This was another reason for the blocking Zone 3 failing to respond to the fault.

The corrective action was to coordinate the sensitivity of supervision and distance elements for both relays (shown as a flag). In addition, the utility changed commissioning testing to check the pickup levels of these supervision settings.

Note that the above scenario and coordination requirements are applicable to a POTT scheme that uses a Zone 3 distance element to block the echoing of the received permissive signal.

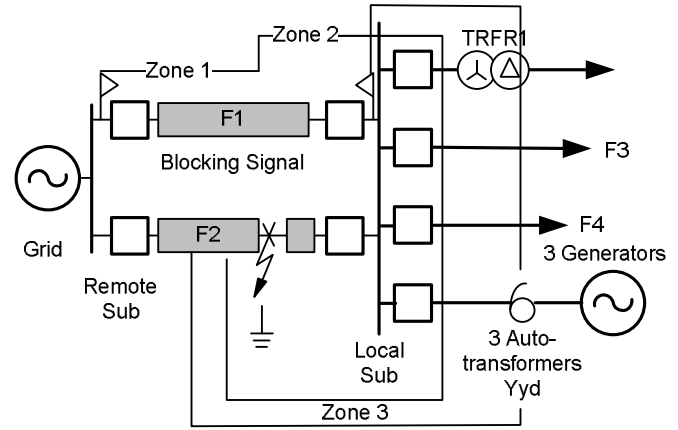
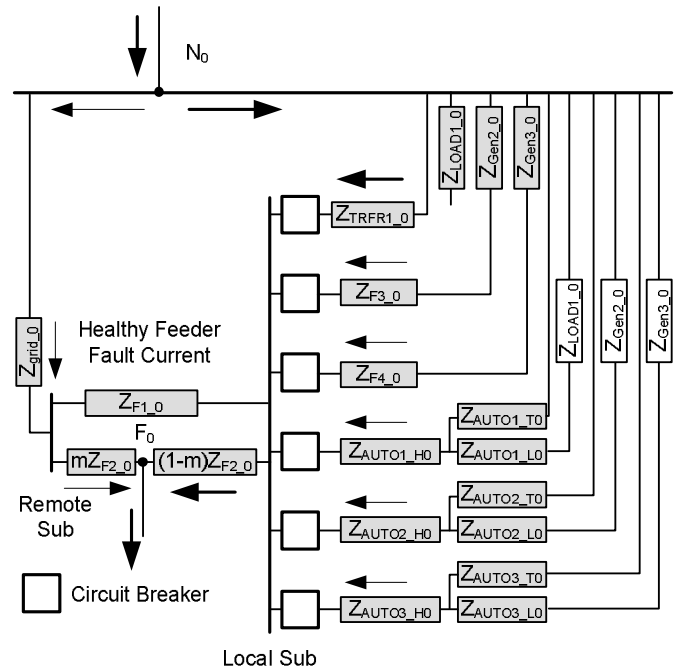


Fig. 1. Local network configuration



Note: Mutual coupling between F1 and F2 is not shown.  
All transformers are solidly grounded.

Fig. 2. Zero-sequence impedance network for a single-line-to-ground fault for the network shown in Fig. 2 (Note that the positive-sequence and negative-sequence networks are not shown.)

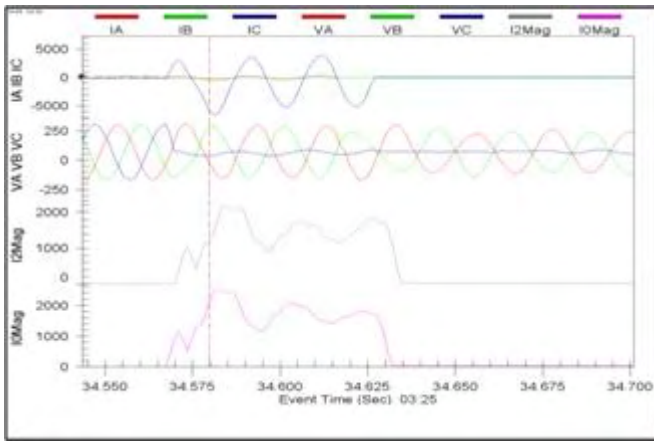


Fig. 3. Unfiltered waveform for faulted feeder's local relay that tripped correctly

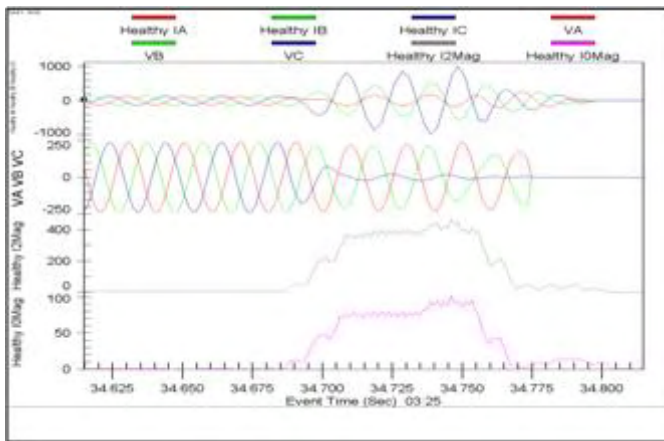


Fig. 4. Filtered waveform for local relay on healthy feeder showing the reconstructed filtered voltages and currents

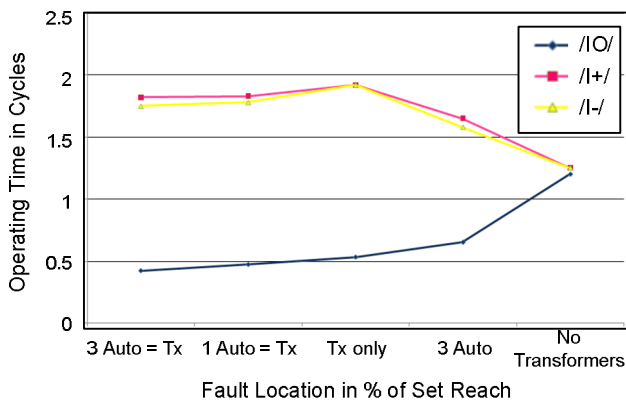


Fig. 5. Sequence current composition in healthy feeder F2 for a fault on F1 at three percent from the local substation

Fig. 5 illustrates, that as the number of transformers increases the zero-sequence current ( $I_0$ ) decreases in the healthy feeder.

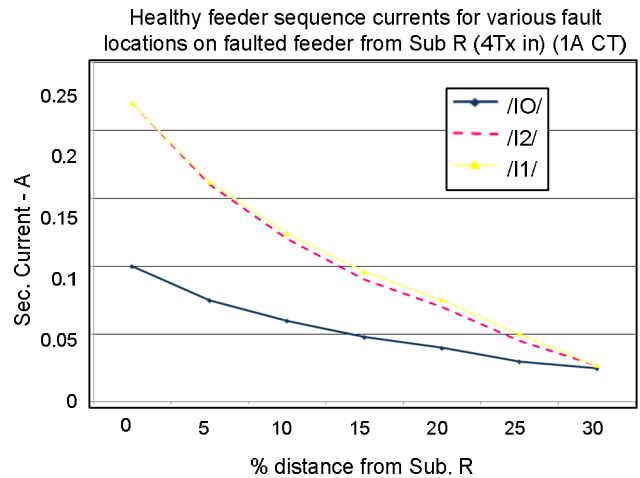


Fig. 6. Sequence current composition in healthy feeder F2 for a fault on F1 at various distances from the local substation

Fig. 6 illustrates that lower values of zero-sequence current flow in the healthy feeder as the fault location approaches the local substation with multiple transformers.

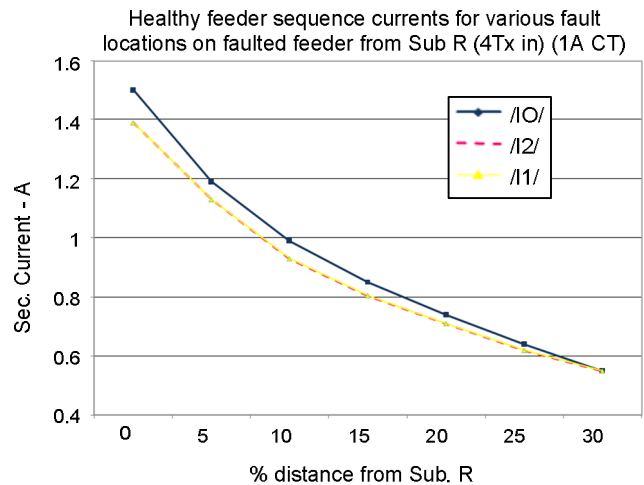


Fig. 7. Sequence current composition in faulted feeder F1 at various distances from the local substation

### 2) Uncoordinated Operating Speeds

The Main 2 DCB scheme used two analog technology distance relays. A numerical relay with high-speed tripping elements operating for Zones 1–3 replaced one of these. A subsequent failure of a surge diverter at the feeder termination within a substation caused this feeder protection to operate correctly. However, a healthy feeder that was contributing fault current tripped at the remote end of its DCB scheme.

An investigation revealed that the numerical relay with high-speed tripping elements picked up 13 ms faster than the local relay. The blocking signal originated with this delay. Although the DCB scheme received the blocking signal 2 ms before the coordination timer expired, the scheme still issued a trip. This unexpected operation resulted from debounce and processing time of the contact input of the remote relay.

The corrective action was to increase the blocking time delay to the maximum value so that it would conform to the AER total fault clearance time. Then, for internal faults, the

Main 1 current differential protection will trip the fault first. The calculated blocking time delays were as shown in Table III:

TABLE III  
BUDGETING FOR THE COORDINATION TIMER OF A DCB SCHEME

	Two High-Speed Relays	Two Conventional Relays
Target Remote-End Clearance Time	6.0	6.0
CB Interruption Time	2.0	2.0
Multitrip Relay	0.25	0.25
Z2 Fault Detection and Trip Output	1.0	1.5
Blocking Timer Setting	2.75	2.25

**Notes:**

1. Time in cycles.
2. It is critical to understand the operation of high speed elements with respect to the applicable zones (1, 2, 3), their “reach”, and time of being active (e.g., 40 ms). The two manufacturers were asked to clarify these points after this event.

### 3) Uncoordinated Distance and DEF Tripping

This case presents the problem where uncoordinated distance, DEF tripping, and reclosing caused the SPAR process to fail. The feeder protection consisted of DCB distance, which initiated single-pole tripping for earth faults, and DCB DEF, which initiated three-pole tripping for earth faults (the relay algorithm did not have fault type identification functionality). The distance and DEF schemes used the same blocking signal and had a 40 ms blocking time delay.

Investigators found that for an end zone earth fault, the Zone 2 distance protection would cause a single-pole trip and start SPAR. Then, DEF protection would initiate three-pole tripping (see Fig. 8). The results were as follows:

#### a) Protection Interaction

- The distance element may reset just before its filtered fault current disappears following the primary current interruption by the CB in one phase. Therefore, the relay logic that blocked DEF tripping during Zone 2 distance element operation released the DEF for operation during the fault current interruption period.
- Then, the DEF element could become active because of the transient nature of the sequence components at that time and issue a trip at the instant that the distance element resets (refer to the red line in Fig. 8).

#### b) SPAR Operation

In addition, the DEF could trip during the SPAR dead time as follows:

- The local and remote relays will block DEF operation (e.g., SPO) internally during SPAR through either CB status signals or internal logic;
- One end of the feeder will reclose first, but current will still not flow in one phase. We know that a pole-open condition will cause the system to have both negative-sequence and zero-sequence current. The magnitude of the negative-sequence and zero-sequence current will be proportional to the load

current and the ratio of the negative-sequence and zero-sequence impedances. The same sequence components appear at both terminals of the line. Therefore, if one element senses in a forward direction, the other senses in a reverse direction. The problem may occur if the terminal that senses the reverse direction has its DEF elements blocked from the open-pole condition while the other terminal already reclosed and reset its block to the DEF element. We can prevent this problem by using a DEF that tolerates the open-pole condition and avoids blocking it under the open-pole condition, or we can key the block signal from the open-pole condition and override it with Z1 or Z2 operation. In this field installation, there was no such remedy.

- Taking into account the way the DEF was blocked under the open-pole condition, the major factors are the time difference in dead times for each end, whether the recloser allows for CB closing time, and latency differences between tripping and reclosers;
- Usually, the relay at the first end to reclose will unblock DEF internally and either send an external blocking signal or wait and then trip on two-phase load current (e.g., a virtual  $I_0$ ). The direction of load current will determine this result. For the installation just described, the common application of blocking signal to distance and DEF functions is detrimental during this interval.

Corrective actions include the following:

- Adjust the application’s single-pole open logic to prevent DEF operation during this interval (see Fig. 9 and Fig. 10);
- Increase the DEF blocking time to 150 ms to prevent a race condition. We can derive this value from network stability limits for substations that have high-impedance faults with a lower  $I^2t$  damaging effect;
- Use relay built-in and user-programmable communications bits from the slave reclose end to send an SPO signal over a digital communications system and block DEF operation during this interval.

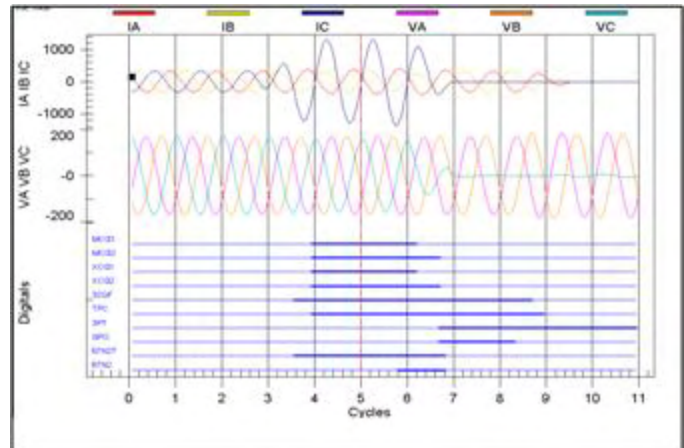


Fig. 8. Sequential tripping path in relay logic for SPT (single-pole tripping = Type 1)

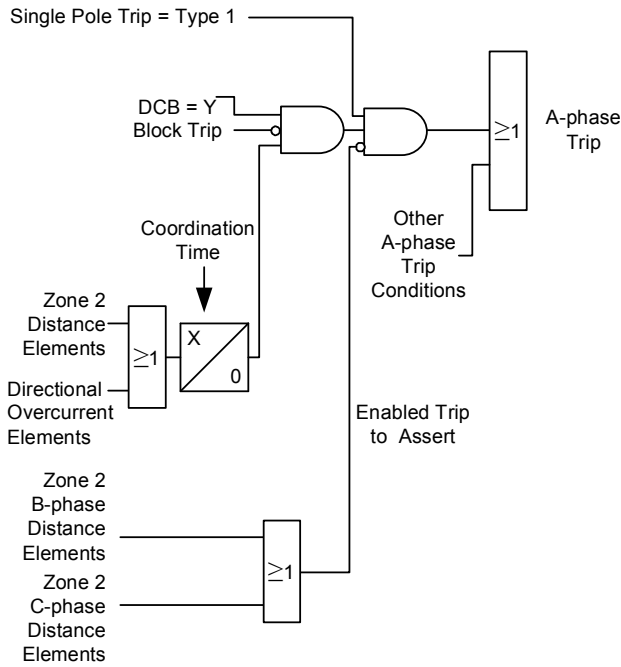


Fig. 9. Simple tripping logic for numerical distance relay (single-pole tripping = Type 1)

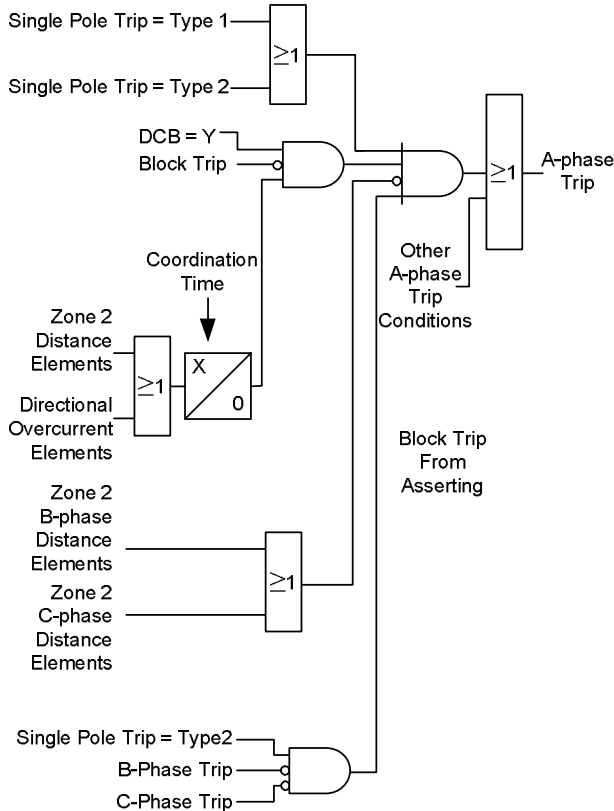


Fig. 10. Simple tripping logic for a numerical distance relay for single pole tripping (single-pole tripping = Type 2; manufacturer recommended relay logic for SPT = Type 2)

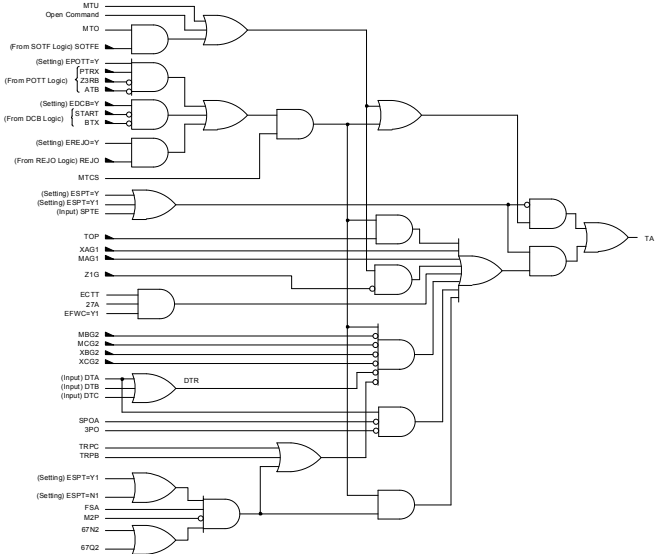


Fig. 11. Detailed tripping logic for a numerical distance relay (A-phase shown only)

#### 4) Uncoordinated Relay Logic

It is critical for logic in numerical relays to be designed with a sequential (numbered) progression of logic gates so that complete processing of an input signal occurs in one scan cycle. When adding a custom logic to standard relay equations, one must be careful to program a given logic engine to minimize latencies resulting from the process of execution.

A protection misoperation occurred, even though the scheme received a blocking signal 10 ms before DEF coordination timer expiration, because the scheme did not process the incoming signal immediately. The application involved a user-programmable logic to augment the standard trip equations of the relay. This modified logic design took an extra 12 ms to process the blocking command, as Fig. 13 illustrates, and issued a DEF trip command. Subsequent testing showed that the relay required between 6–12 ms to recognize and act upon a blocking signal input (the relay response time varied as a result of the time the signal arrived within the relay scan cycle of the inputs (latency), debounce filtering, and logic gate precedence). Optimizing the user-programmable logic in terms of logic gate sequence in the execution cycle reduced this time range by 5 ms.

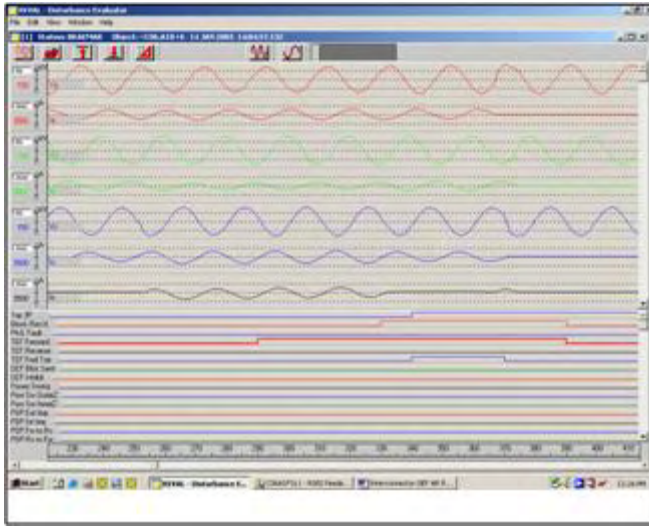


Fig. 12. Nonoptimum design of a user programmable logic resulted in extra delay in receiving the blocking signal

### 5) Communications Delay

It is critical for increasing the margin of safety that the DCB scheme send the blocking signal rapidly over the communications system. In one utility, investigators discovered that the communications group had specified that blocking signal propagation delay must be 15–20 ms (in accordance with direct transfer tripping requirements). For faster digital communications systems, the communications group delayed the blocking signal intentionally to comply with this range. Fig. 13 illustrates the point at which the scheme received the blocking signal 2 ms before the timer expired. This case illustrates the need for better training and clarity in stating equipment or service requirements, particularly when multiple disciplines or departments are involved.

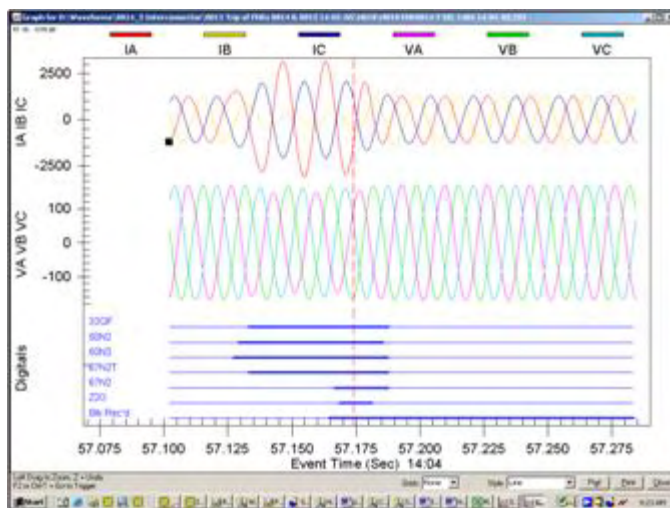


Fig. 13. Record 5 illustrates the point where the blocking signal was received 2 ms before the timer expired.

## V. IMPORTANCE OF TESTING

The previous field cases demonstrate the importance of effective setting practices and testing with the correct fault quantities. One very important result from these events was

education for protection and test staff on how these events occurred and on how to be more effective in their work.

### A. Testing Coordination

DCB scheme testing usually involves independent testing of each relay and a loopback test of the communications system. Then, if these results conform to the designer's requirements, testers can assume correct scheme coordination. The reasons for this simple testing are as follows:

- The protection designer should ensure coordination of the two relays based upon fault studies for various scenarios. For demanding cases, or for applications of new relay models, testers should perform specific tests (with appropriate test quantities specified). Such tests would involve use of closely modeled system conditions such as from playback of electromagnetic transient program files, a real-time digital simulator (RTDS), or information from testing staff who used fault study or historical record values (see Section V. Importance of Testing). Afterwards, the designer should obtain test results and confirm coordination;
- Past experience with independent end testing (each relay in the scheme tested separately) shows such testing to be very successful for achieving scheme performance. However, the principal aim of this testing was to confirm that the applied relay settings achieved the designer's operating or speed requirements at specific point(s). Such testing does not cover the wide spectrum of possible fault conditions and fault transients. Also, it is critical to remember for numerical distance relays, that pickup tests of supervision and distance elements must be performed;
- It has been difficult in the past to coordinate end-to-end testing, end-to-end testing is costly and requires the use of two crews, and there is a reluctance to remove protection systems from an in-service feeder (in eastern Australia, for example, eight hours is the maximum time a protection system can be isolated on an in-service feeder);
- The loopback test of the communications system measures twice the propagation delay time for a blocking signal. Usually this time must be less than a specified maximum value.

### B. Post-Fault Analysis

One critical test is to check the blocking safety margin of a DCB scheme for a healthy feeder(s) contributing current to a fault on an adjacent feeder. Unfortunately, all of the attention focuses on the faulted feeder, and performances of the contributing feeders are ignored. This margin equals Zone 2 pickup time plus blocking duration time and minus blocking signal receive time. The scheme records these times in the disturbance or event records of the numerical relay or in the records of the substation SCADA. It is good practice to check the safety margin for each relay that picked up its Zone 2. We can derive the time difference between Zone 2 pickup and when the scheme received the block after automatic readout via SCADA records and then compare this value to the set

coordination timer. We can then fine tune the scheme for best security. A change in the margin after an initial observation period can signal changing system conditions that we can use to trigger review of settings or retest of communications equipment and/or relays. Note that scheme performance will usually be different for each end because of the different relays and different fault levels in use.

### C. Playback Testing

Today, it is simple and effective to replay recorded disturbance records through RTDS or microprocessor-based test equipment. The protection designer must actively collect these records for faulted and healthy feeders to enable future evaluations of new relays or scheme performance. Obviously, the protection designer must set the relay's disturbance recorder to operate as follows:

- Trigger on and record pickup of zone elements, blocking send/ receive signals, supervision and fault identification elements, tripping outputs, etc. The example in Fig. 14 shows that comprehensive recording of external inputs and internal signals in a numerical distance relay used only 37 percent of capacity;
- Record unfiltered quantities at a rate of at least 800 samples per second;
- Provide COMTRADE format files (where possible).

Without this recording, an investigation could be difficult and time consuming. This is because, in a majority of cases, the cause of an unwanted DCB scheme trip is at the blocking end. This end does not trip, and it sometimes does not even detect the reverse fault. Therefore, the recording trigger at this end must be more sophisticated and include sensitive reverse and/or nondirectional elements such as negative-sequence overcurrent or overvoltage, or disturbance detectors. With reference to Section IV. Sample Field Cases, the disturbance records for faulted feeders are not applicable to testing relays on the healthy feeder. This is because the zero-sequence current composition will be different. In addition, it is important that there be at least several cycles of prefault waveform so that the distance relay polarizing quantity stabilizes at an in-service value. Appendix 6: Troubleshooting Field Cases describes a process to convert disturbance files into COMTRADE format and then cut and paste two disturbance files into one. We used this process to fabricate a test file for the local relay on the healthy feeder.



Fig. 14. Example of setting recording digitals for a disturbance recorder

### D. Real Time Digital Simulator Testing

Before commissioning any important feeder into service, many utilities require extensive transient fault studies to verify the performance of the protection system and to validate the applied settings under actual system conditions. To meet these requirements, an accurate model of the power system is built in a real time digital simulator (RTDS). This model includes not only the primary power system equipment such as the power transformer, feeders etc, but also the instrument transformers such as the voltage/potential transformers (PTs) and current transformers (CTs). RTDS output signals such as the secondary current and voltage and CB status are inputs into the relay. Relay outputs such as the trip and reclose signal are fed back into the RTDS, thereby forming a closed loop similar to a real power system.

Fig. 15 shows the closed loop RTDS testing scheme.

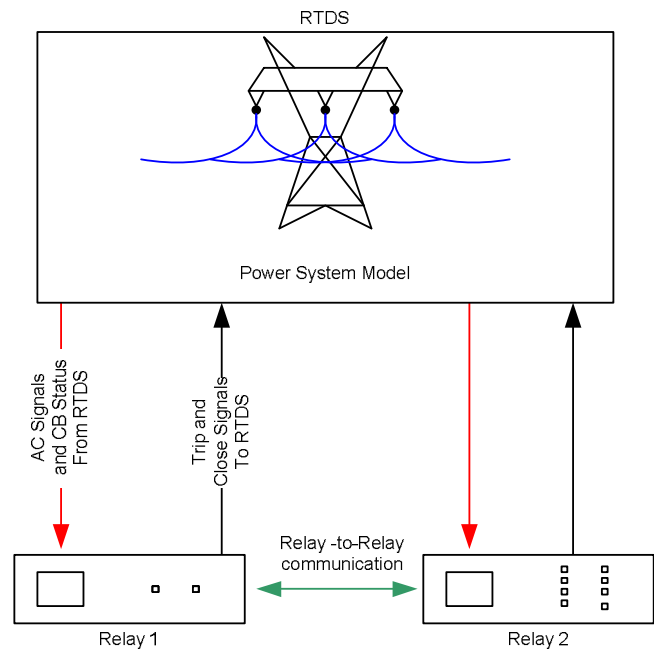


Fig. 15. Simplified sketch of an RTDS simulator testing setup

We first verify the RTDS model against power flow programs such as PSSE™ and power system transient programs such as EMTP™. Once we complete this verification, we use conventional fault calculation programs

such as ASPEN™ or CAPE™ to obtain the preliminary settings.

Before we proceed, it may be a good time to ask, “Why bother with all this? Why not just use the data we obtained from the fault study programs, apply the settings to the relay, and call it good?”

Consider the following:

- Fault study programs often only output the steady state current. For example, when faults are close to generators, these programs ignore the effects of the subtransient and transient impedance of the generator and only consider the steady state impedance;
- Fault study programs ignore the point on wave (voltage) when the fault occurs, they therefore do not consider the dc offset of the fault current;
- Fault study programs do not include the effects that instrument transformers can have on the signals entering the protective devices;
- Fault study programs do not indicate how the protective relay will perform under different fault conditions.

Now let us focus on DCB scheme performance for faulted and healthy feeders. The following are two interesting cases that occurred during RTDS testing.

- The local and remote relays had different types of CTs (not an uncommon practice). Testers simulated an external fault just behind the remote terminal relay. The remote relay detected the fault in the forward direction. The local relay detected the fault in its Zone 3 and sent the blocking signal as expected. Approximately 2.5 cycles into the fault, however, the local CT experienced mild CT saturation (as a result of dc offset). This saturation was enough to deassert the Zone 3 blocking signal, and this deassertion of the blocking signal resulted in the local Zone 2 tripping for an external fault. It is true that in most cases CT saturation affects dependability of distance functions, not security (causes underreach not an overreach). However, an underreach of a reverse-looking Zone 3 used to block a DCB scheme leads to a loss of security. The solution was to add the reverse negative-sequence directional element to the blocking logic. This caused the blocking signal to remain asserted. Fig. 16 shows the sequence of events that resulted in the unwanted trip.

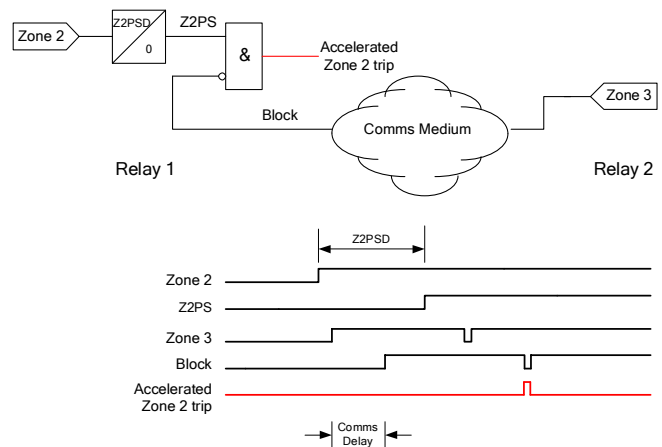


Fig. 16. Simplified sketch of a DCB scheme and a sequence of events that could lead to an unwanted DCB trip

- A dual circuit parallel feeder application that employs single-pole tripping uses two similar distance relays, one at each end. Through the use of the maximum carrier delay plus the relay contact input and output times, testers correctly calculated the coordination timers, and the protection operated correctly for external faults.

The problem occurred for in-zone fault testing. The fault began as a close-in C-phase-to-ground fault on the Feeder 1 terminal. Within the first cycle, the fault evolves into an inter-circuit fault with a C-phase-to-ground fault on Feeder 1 and an A-phase-to-ground fault on Feeder 2. This scenario can simulate a bushfire or back-flashover of insulators resulting from lightning strikes on unshielded dual circuits.

Fig. 17 shows the fault scenario and the fault current distribution. The result was that a single-pole trip (SPT) occurred at both local terminals, and a three-pole trip (3PT) occurred at the remote terminals, effectively isolating the system. The problem was that the local relays saw the faults as single-phase faults. The overreaching distance elements (Zones 2) for the remote relays correctly saw the faults as phase-to-phase faults. This is to be expected because the remote relay had depressed voltage in two phases and associated fault current in two phases.

The possible solutions include the following:

- Increase the Zone 2 blocking delay (delay tripping of the remote relays) and allow the local breakers to trip first. When the local breakers trip the remote relays, fault identification logic now detects the fault as a single-line-to-ground fault. The fault identification logic will deassert the phase-to-phase distance element, enable the single-phase distance element, and correctly isolate the fault.
- Use standard blocking delay and send a blocking signal from local relays while tripping for each circuit with different phase-to-ground faults. This has the same effect, but there are no delays for single-end zone faults for this special scenario. This requires that the scheme send multiple blocking signals, not a problem when the scheme uses built-in digital

teleprotection solutions (e.g., MIRRORRED BITS<sup>®</sup> communications).

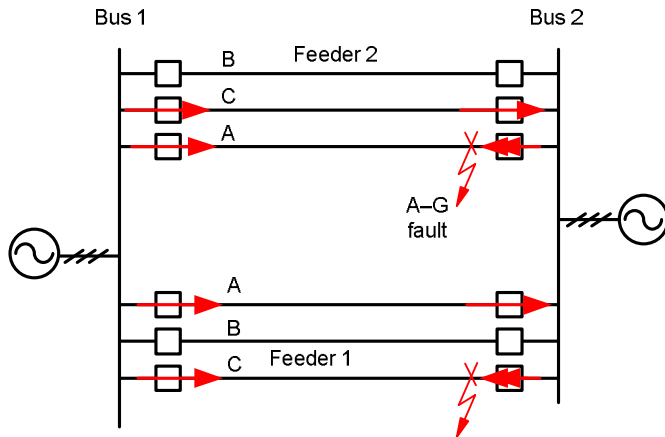


Fig. 17. Fault scenario and the fault current distribution

From these two events, we can readily see that RTDS testing prevented two possible DCB scheme misoperations. A further advantage of this type of testing is that it can be used to capture COMTRADE files for both feeder ends. It would then be possible to use these files during commissioning to do synchronized end-to-end testing of the actual feeder.

## VI. ENHANCEMENTS TO DCB SCHEMES

### A. Introduction

We present in this section the impacts of intelligent electronic devices (IEDs), digital communications, and electricity market considerations with respect to DCB schemes. We raise in this paper the question of whether either permissive transfer tripping schemes or current differential protection (with a suitable backup strategy) can supersede DCB schemes as a first choice protection. Obviously, the new scheme must provide similar performance. The benefits of dependable, digital communication and numerical relays with communications failover functionality, backup protection, and flexible relay logic capability are key enablers for this ongoing evolution in protection policy and application. The following text presents various factors shaping this strategy.

### B. Network Factors and the Electricity Market

The following are critical factors (refer to Appendix 9: Present Environment and Digital Communications for detail):

- Electricity is now fundamental to standard of living, and society demands 24-hour, seven-day-a-week availability;
- The electricity market and regulators have evolved. AER has taken a proactive approach to driving electricity prices down through rewarding efficiency (e.g., security of supply bonus/ penalty payments of as much as  $\pm$  \$5M) and setting income rates, capital, and operational expenditure for transmission companies;
- Protection engineers provide a valuable service to society by providing a reliable supply of electricity,

and as society's expectations change, engineers should review and improve this service. In addition, utility management teams learn quickly if a protection misoperation occurs and see its impact on the bottom line.

- The electricity network has expanded, and this increases the network infrastructure that enables additional communications routes;
- Digital communications networks and OPGW offer new protection opportunities and excellent performance. Results include very reliable protection signaling; increased number of signals; and possibly redundant, independent paths for the vast majority of feeders. One emerging problem is path switching, which could impact teleprotection (see Appendix 9: Present Environment and Digital Communications);
- Numerical current differential relays with the capabilities of backup protection (distance, directional, overcurrent), GPS time-referenced sampling, and redundant communications ports.

Let us now examine the DCB protection scheme from within the framework of a challenging electricity market environment and network growth.

### C. DCB Scheme Fitness for Purpose

This scheme's principal advantage was its ability to send a signal over the unfaulted feeder. This was important in the past where analog PLC communication was in widespread use and where the signal could be highly attenuated, become noisy when propagated through the fault, or when conductors broke or melted. Digital communications systems and the capabilities of numerical relays minimize the principle advantage of DCB schemes.

Block tripping is one disadvantage of the DCB scheme in terms of security for healthy feeders supplying faults. We can describe this as double jeopardy, where one event can cause multiple line outages and lead ultimately to customer loss of supply or network instability (see Appendix 9: Present Environment and Digital Communications).

Walter Elmore at PAC in the summer of 2007 said, "To accept something the way it's always been done is not acceptable. There is too much of that—accepting things the way they are."

So protection engineers must now ask, "Is there a better way than DCB, given advancements in communications channels?" They must also still consider, however, the principle that, "Dependability of protection operation has precedence over security of supply."

Ian Stevens suggests, "The modern ART of Protection is intelligently using technology to get dependability and optimum security!"

### D. Dependability of a Line Protection Scheme

This section examines strategies for achieving dependable line protection. The basic components for dependable scheme operation are as follows:

- A protection system that detects any internal feeder fault and then trips the correct system so that all systems can be made secure (refrain) for external feeder faults. To ensure this for transmission assets, system designers employ duplicated protection schemes with different operating principles and use numerical relays from different manufacturers (in an attempt to overcome common failures).
- Dependable communications systems for teleprotection. Obviously, cost, type, quality, availability, and redundancy of communications equipment and systems determine the application strategy.
- The need for each critical component to have a self-diagnostic function to assert alarms for failures or switch communications paths before they must operate. These are critical benefits of digital technology.

Duplicated protection schemes require two independent communications systems. Assuming that one system could use OPGW, the remaining system could use the following:

- A different fiber within OPGW. This is not the best practice because of the possibility of common mode failure. Two following examples show where a fiber splicing box filled with water as a result of porous seam welds. The water eroded the fibers' aluminum tube, and this resulted in compressed fibers and grossly attenuated signals.
- An alternative route via a third feeder or a composite route through multiple feeders.
- Use of two OPGWs on the same route. This could be acceptable for short feeders.
- Other communications media such as microwave, radio, leased lines, etc.

There is debate within the protection community about whether the use of two OPGWs on the same tower provides true independent and redundant protection schemes. Appendix 9: Present Environment and Digital Communications and the conclusion provide a reliability assessment of fiber communications media. Such media are not absolutely reliable for protection duty on long feeders, but they can be designed and installed to be more reliable than analog PLCs.

The previous considerations show the necessity of an integrated solution of quality communications systems (hardware, design, installation, redundancy capability) and an intelligent redundancy strategy in the numerical relay. Protection engineers must therefore have the following:

- A competent understanding of digital communications systems, their dependability, and their evolving characteristics;
- A working relationship with communications engineers to realize these advantages.



Fig. 18. A failed FO splicing box showing the rusted stand broken from the base and aluminum tube corrosion that caused pressure on fiber, high-signal attenuation, and failure of the communications system

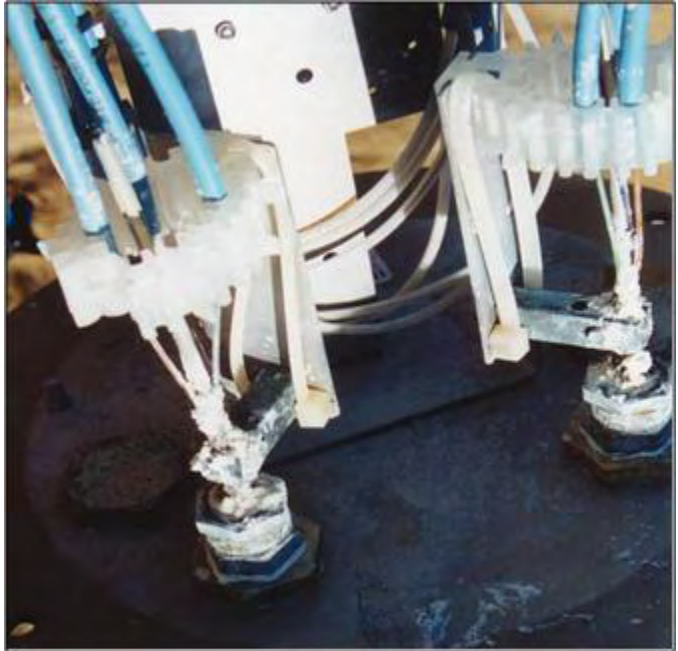


Fig. 19. A failed FO splicing box showing how corrosion exerted pressure on fiber and high-signal attenuation caused the communications system to fail

#### E. Strategy

The strategy is to use a standard scheme and inherent hardware capabilities (keep it straight and simple principle, then test for fallibility) to only add the minimum functionality.

The goals are as follows:

- 100 percent redundancy as per the DCB scheme, but perhaps slightly slower tripping as to grade.
- Where practical during a communications failure, compliance to AER total fault clearance time or, by applying the contingency rule, allowance of 16 hours to repair a failure before isolating the feeder.
- Improved security by reducing the tripping of healthy feeders.

The approach:

- Use Failure Mode Effects Analysis on the standard scheme to determine the modes of failure for protection and communications subsystems. Obviously, the types of available communications carriers and their redundancy capabilities will be pivotal for each feeder's teleprotection, so it is a good idea to discuss requirements with communications

engineers. For this utility, OPGW and microwave carriers, SONET/SDH and alternate routes are available.

- For each failure mode, determine when and how it occurs, its probability, and options to overcome it. Appendix 9: Present Environment and Digital Communications examines the modes for OPGW and SONET/SDH redundancy.
- Determine the usable attributes of the line, SPT or 3PT, numerical relays, and protection policy. For example, an overreaching distance element provides backup. Because numerical distance relays have an accuracy of  $\pm 5$  percent, and the errors for CT/VT are less for end zone faults, it may be acceptable to extend Zone 1 to 90 percent and reduce Zone 2 slightly (only during communications failure). Changing settings groups can accomplish this.
- Consider maintenance requirements for protection and communications subsystems.
- Determine grading requirements with adjacent protection systems (stepped distance protection). Usually there are two possible responses when the communications system(s) becomes unavailable.
- Enable fast Zone 2 tripping for a short period (say 10 cycles for any possible catastrophic event that could cause a fault) and then establish a graded Zone 2 time delay.
- Enable Zone 2 to trip after the remote substation's primary protection has cleared the external fault (say six cycles). You could, for example, have protection grading and a margin with a time of 7.5 cycles. (**Notes:** Zone 1 faults trip immediately; standard Zone 2 time operation remains unchanged.)

The protection engineer must decide when and how the relay will respond to ensure dependability.

- Determine the cost sensitivity for options and potential benefits of increased security. Because protection systems comprise about 2 percent of project cost for a new substation, the cost sensitivity should be low unless a "lean and mean" culture exists. Senior management can appreciate a tangible dollar value for security.
- Design the simple add-on to achieve the goals. Determine the tradeoffs between dependability and security (i.e., tripping for external faults) and optimize. It is important that the relay record and indicate its operating mode with front-panel indications. This is an important aid for test staff.
- Document the design and get a design review by an experienced protection engineer and test engineer. Create a test plan from a scheme functional/operational mode matrix.
- Test the scheme for compliance, failure, transfer, and recovery modes. The teleprotection signals should use an actual communications system(s), and tests should include its degrading and failure modes. Our helpful communications staff provides such equipment with a

1000 km loop into their network and back to the test domain.

- After successful testing, fully document the scheme, apply version control, and train relevant staff. Ensure that the scheme's manual will be available in each substation that uses the scheme. Remember that this scheme will probably be in service for 15–20 years.

#### F. Permissive Transfer Tripping Scheme

Based upon the above reliability conclusion for digital communication and a greater security of supply incentive, utilities may consider changing from DCB to POTT as the preferred distance or directional teleprotection scheme. There are three advantages from using a POTT scheme:

- Coordination of protection settings and switching communications channels are less arduous than for the DCB scheme.
- There is a considerably smaller risk of tripping healthy feeders.
- Distance teleprotection is more tolerant of communications route switching than is current differential.

Let us use the following duplicate teleprotection scheme information to develop an illustrative strategy:

- Main 1 will be first generation current differential (with two distance elements) and OPGW or SONET/SDH.
- Main 2 will be numerical distance that uses a POTT scheme and available communication.
- The scheme will use single-pole tripping, except where stated;
- All signals have independent ports on each carrier. The digital SONET/SDH will have 1+1 redundancy, and an alternate route will have 1+0 redundancy. Communications route redirection is available.

Salient points of design:

Main 1:

- OPGW route is satisfactory for current differential because it has a propagation delay of less than 10 ms. Checks of alternate routes and signal rerouting show that they are unacceptable.
- If a fiber path fails, the multiplexer seamlessly switches to the duplicate fiber. If the duplicate fiber now fails, the OPGW communications system fails and alarms.
- The backup protection for the relay was set as POTT. It will operate over the alternate route with, say, a 40 ms propagation delay. A check shows that the total fault clearance time is compliant in this mode. If a component in this route fails, the relay provides dependable tripping until the feeder is isolated.

Main 2:

- To improve scheme dependability, permissive signals will be sent via OPGW and an alternate route. Checks show that the total fault clearance times are compliant in both modes. The contingencies of Main 1 are applicable.

- The design accommodates the sequence of communications failures and maintenance impact.
- For either communications system's failure, duplicate POTT schemes are operational on a common system although compliant tripping will occur. AER requires independent schemes, so it is possible to apply the contingency clause while performing repair.

For failure of a remaining route, we can apply the capabilities of the numerical relays strategically:

- Zone 1 remains at 80 percent reach, and the scheme trips a fault immediately as 3PT.
- Zone 2 remains at 120 percent reach. Enable an additional Zone 2 time-delayed trip output for 3PT. Select the time delay to grade during the remote substation's primary protection fault clearance (a worst case of four cycles, for example). This would mean protection grading and margin with a time delay of 5.5 cycles but within stability limits. The standard Zone 2 time operation is not altered. Here are the protection responses:
  - For an external fault: Zone 2 sees it but waits, and remote protection correctly clears the fault;
  - For an internal fault: local end Zone 1 trips immediately as 3PT; remote end Zone 2 waits 5.5 cycles, initiates tripping, and clears the fault after 7.5 cycles (two cycle CBs) after starting.
  - For an external CB failure event: Zone 2 clears as before in 7.5 cycles, which beats the external CB fail protection operation (10 cycles, for example). For a Teed feeder, this could result in loss of supply. However, CB fail events are rare.
  - Any auto-reclose function will be disabled in this state.
  - With no communications systems available, the control center will isolate the feeder until a communications system can be repaired. Note that this is a worst-case scenario, but it is one we must consider.

The above design has achieved 100 percent dependability with an insignificant risk of Zone 2 incorrectly tripping for an external fault. The incremental cost for additional functionality will be about 5 percent of teleprotection's capital cost.

Obviously, we must consider this solution in holistic terms of communications infrastructure and route switching, customer or load requirements, alternate supply, system maintenance, cost etc.

The authors invite the protection community to send them comments on this strategy.

## VII. SUMMARY

### A. Important Lessons Learned

The following summarizes good practice and lessons learned from the DCB scheme field cases.

- Sensitivity and detection speed of the local and remote relays must be coordinated for zone protection

characteristics and supervision functions. This ensures that the local relay will send a blocking signal for any external feeder fault that the remote relay can detect. Sensitivity in this aspect relates to both settings and operating principles. The evidence of failed coordination is tripping at the remote end of healthy feeders. Configure recording triggers carefully to ensure that evidence is available for quick troubleshooting and fine tuning of applications that failed.

- Where possible, maximize the blocking time delay to give acceptable performance against mandatory fault clearance time and/or network requirements. The operating performance of the duplicate protection will impact this time selection. This can allow tripping of the faulted feeder before the healthy feeder(s) can be jeopardized.
- Where possible, use two blocking signals on independent communications systems, and use either one to block tripping execution. Give consideration to monitoring the systems' GUARD status and having SCADA alarms for failure of any signal circuit.
- Ensure that there is no additional delay inserted into blocking signal propagation by either communications practices or circuitry (e.g., use of slow or contact-bouncing armature relays).
- For multiple transformer substations with direct-earthed Yd transformer types, ensure that the fault studies include a reverse bus fault and check/test the veracity of the first point.
- Set the disturbance and event recorders to maximize fault information to enable effective checks of tripping and blocking operations for faulted and healthy feeders.
- Where possible, use a shorter blocking time delay for distance elements that detect high-energy faults, and use a longer blocking time delay for DEF elements that detect low-energy faults. This ensures coordination.
- Perform testing of DCB schemes based upon fault studies, historical data records, or RTDS to check correct scheme operation for tripping and blocking modes. Typical test cases include impact of relay supervision functions, SPAR, new model of relay or technology, and special applications. Note that the authors are unaware of any Teed application of a DCB scheme.
- Ensure that you understand the impacts of new technology or protection algorithms completely and that you know how to test them effectively. It would appear that the utility and the manufacturer for high-speed and supervision functions did not achieve this.. The utility must realize that manufacturers, to protect their intellectual property, may not disclose all relevant information in the relay manual, and a simple relay upgrade in a scheme can compromise scheme performance.

### B. Electricity Market

The introduction of an electricity market can require intelligent design of protection systems so as to achieve more dependable and secure performance. The tripping of healthy feeders during a fault may affect the electricity market, and such tripping can cause a utility to incur financial penalties and questioning by the market's regulator.

Be aware of the impacts of load growth and resulting network augmentation, advances in communications systems, and increased functionality of numerical relays. You can apply these factors toward improving the performance of teleprotection schemes;

New generation, renewable in particular, can be non-standard short-circuit sources. Short-circuit models may be still under development and cannot be trusted fully. Some protection principles can respond marginally for such sources. Permissive schemes or line current differential schemes may be a better choice for systems with a higher number of non-standard short-circuit sources.

From the previous discussion, it should be apparent that protection engineers must reconsider the suitability of DCB scheme and accordingly provide a better alternative or an improvement to security. We presented here a strategy in which we processed communications system failures to achieve dependability and security.

### C. Evolution

We reviewed and illustrated in this paper several aspects of communications-assisted line protection.

The art of such protection is satisfying the conflicting demands of dependability and security through a design that takes into account application of digital technologies within a rapidly changing environment. The environment includes the electricity market, the regulation of capital projects and their cost, the increased visibility of protection misoperation, the need to refurbish aged assets in substations, and the impact of network growth upon protection systems. In addition, there remains a need to integrate more successfully knowledge of protection and communications.

## VIII. APPENDIX 1: TYPES OF TELEPROTECTION SCHEMES

We have provided the following information for less experienced protection engineers to learn about teleprotection schemes. We expect that the reader has a basic knowledge of distance relaying.

There are three types of basic communications-assisted tripping schemes:

1. **Direct Transfer Trip Direct (DTT)** –In this scheme, in a manner similar to the relay that initiated the DTT [2], the relay uses any local currents or voltages and instantaneously trips on receipt of the signal without any qualification or verification. Typical applications include remote breaker failure, blind spot tripping, transformer-ended feeder, and situations in which a weak source feeds one line end and its relay may not see a feeder fault because of high infeed from a strong source at the other line end. In this case, application of

DTT initiates tripping of the relay at the weak terminal. Fig. 20 is a simple sketch of a DTT scheme on a system where one source is much stronger than the other. An underreaching Zone 1 at the strong line terminal initiates the DTT.

It is also possible to perform direct transfer tripping on a per-phase basis. Again, if a weak source supplies the remote terminal, the terminal may not have sufficient voltage and current to correctly identify the faulted phase. Therefore, to avoid compromising single-pole tripping, per-phase direct transfer tripping is employed [3]. Because the remote end does not verify the received trip signal, the communications channel must be adequately secure to prevent an inadvertent transient on this channel that could cause an unwanted trip.

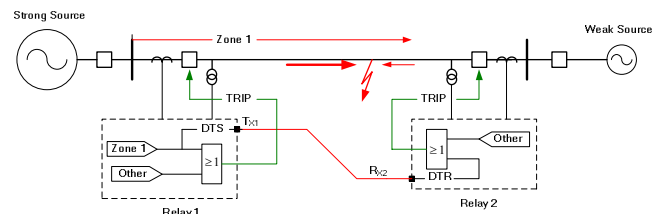


Fig. 20. A simple sketch of a DTT scheme

2. **Permissive Transfer Trip (PTT)** – The scheme operation differs from the DTT scheme as follows:
    - The local relay sends a signal if it detects the fault in its forward-looking zone;
    - Upon receipt of the signal, the remote relay checks to see if it meets the criteria for tripping in Zone 2. For a valid check, it is necessary to bypass the Zone 2 timer to trip for an internal feeder fault. Otherwise, the Zone 2 timer must operate to trip and time grade for an external fault (e.g., CB failed in the remote substation).
- A fault within Zone 1 causes this zone to trip immediately.

Because the relay qualifies the signal before accelerating tripping, the scheme is more secure than the DTT scheme. We can realize this scheme in one of two ways:

- Permissive Underreaching Transfer Trip (PUTT) scheme and
- Permissive Overreaching Transfer Trip (POTT) scheme

The initiation source of the carrier signal discriminates these two schemes from each other. In a PUTT scheme, as the scheme name indicates, the underreaching element (Zone 1) keys or transmits the signal. Fig. 21 is a basic representation of a PUTT scheme. One disadvantage of PUTT is the reduced arc coverage of the Zone 1 element.

In a POTT scheme, as in Fig. 22, the overreaching element (Zone 2), which has larger arc coverage, keys or transmits the signal. The POTT scheme uses the overreaching element to send a permissive signal, so it

must have a reverse looking zone to block the remote end from echoing a permissive signal back to the local relay for a fault external to the feeder. The PUTT scheme does not need this zone because the underreaching zone never sees past the remote end of the feeder. Further discrimination between the two schemes is that the POTT scheme must have a third distance zone set to look in the reverse direction. This zone is necessary to prevent the remote end from echoing the received signal back to the local end, if the remote relay detects the fault behind it (i.e., the fault is external to the feeder).

Permissive schemes are biased toward security of supply, rather than dependability of protection operation. This means that if the communications system is unavailable, then the remote relay will trip in Zone 2 time (delayed) for a fault close to the local relay, but it will remain stable for external faults. Security of this channel is not as important as for a DTT scheme because an inadvertent signal (e.g., transient burst on the communications channel) will not lead to inadvertent tripping. The major disadvantage of PTT in use with communications channels associated with the protected line (PLC or OPGW) is that the signal must pass through the fault. This could be difficult for analog PLC or become problematic if the line loses mechanical integrity in addition to having an electrical short circuit (as could happen, for example, with aircraft accidents impacting ground wires and embedded fiber).

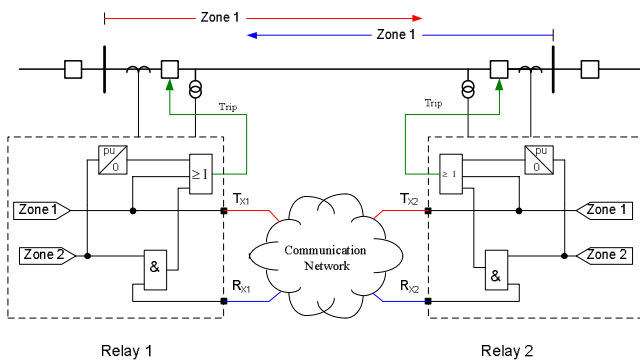


Fig. 21. A simplified sketch of a PUTT communications-assisted tripping scheme

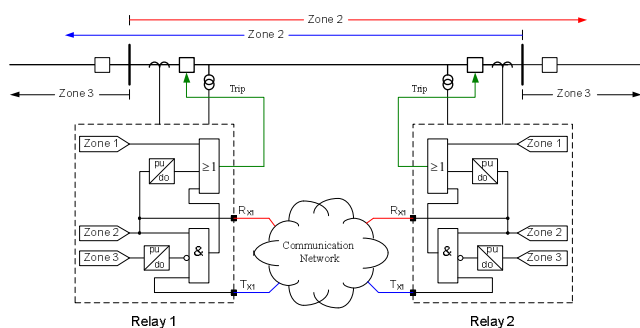


Fig. 22. A simplified sketch of a POTT communications-assisted tripping scheme

3. Directional Comparison Blocking Scheme (DCB)— Operation of this scheme is the opposite of permissive scheme operation:

- **Feeder fault in Zone 2:** The remote relay detects a fault in Zone 2. If it does not receive a signal from the local relay within a preset time, it trips instantaneously (accelerated tripping compared to a stepped distance timer).
- **Fault external to feeder but in Zone 2:** The remote relay detects a fault in Zone 2. If it receives a signal from the local relay within a preset time, it delays tripping to Zone 2. The local terminal should only send a signal if it detects the fault in the reverse direction (typically Zone 3).
- **Feeder fault in Zone 1:** The relay trips instantaneously.

In other words, as the scheme's name indicates, the transmitted signal is a blocking signal. This scheme differs from the permissive scheme in that it sends a signal if it detects an external fault within Zone 3. The permissive scheme, on the other hand, sends a signal if it detects the fault within a feeder's protective zone (Zone 1 or Zone 2, depending on the type of scheme selected).

Fig. 23 is a simplified sketch of a DCB communications-assisted tripping scheme. Assume that you have a fault within the protected feeder and that the communications medium is compromised. There will be an accelerated clearing of the fault (which is what we want). However, if the fault were directly behind the local relay, and the remote relay detected the fault within its protective zone (Zone 2), the remote relay would trip quickly for an external fault because the blocking signal did not reach the remote relay (we do not want this response). Therefore, this scheme is biased toward dependability of protection operation rather than security. To improve security of supply, DCB usually employs duplicate blocking signals and enabling through the channel OK (guard function) signal from the communications system. The major advantage of DCB is that the signal does not pass through the fault. Its operation and speed are therefore assured.

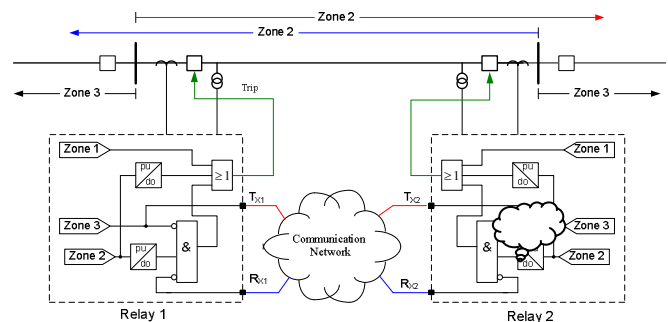


Fig. 23. A simplified sketch of a DCB communications-assisted tripping scheme

In applications on multiterminal lines, any terminal that issues a block inhibits the entire scheme. Therefore, for applications that use PLC, all terminals could share the same frequency (channel) to block the scheme. For any given external fault, only one relay should transmit the blocking

signal; for any given internal fault none of the relays should transmit. This is yet another advantage of DCB over PTT for systems that use PLCs.

For the sake of completeness, we will mention but not explain in detail in this paper a fourth type of communications-aided tripping scheme that is in essence a subset of the permissive transfer trip scheme. This scheme, known as a directional comparison unblocking scheme (DCUB), must receive a carrier signal from the remote end and a deasserted guard signal from the communications equipment before it will operate.

## IX. APPENDIX 2: SELECTION OF BLOCKING SCHEME

As we stated in Appendix 1: Types of Teleprotection Schemes, we employ a teleprotection scheme to create a pseudo unit protection scheme that uses distance or directional relays. Under ideal conditions with all protection and communications functions working correctly, there is no difference between a blocking or a permissive scheme. The decision whether to use a permissive scheme or a blocking scheme has consequences for the overall performance of the scheme if one considers certain failure modes in the relaying or communication parts of the scheme. Examples of problems causing different impacts for a permissive versus a blocking scheme include a failure of a protection element to pick up, communications delay beyond the expected value, and a spurious or missing communications signal. The following is a brief discussion on the criteria necessary for selecting the scheme type.

Principally, the type, availability, and cost of communications systems greatly influence scheme selection (see Appendix 9: Present Environment and Digital Communications). However, protection engineers can prescribe requirements based upon their needs to:

- Clear all foreseeable faults so as to maintain network stability;
- Minimize HV plant/feeder damage;
- Minimize the area of supply interruption, therefore ensuring public safety.

Essentially, reclosing an incorrectly tripped feeder is much more preferable than unlimited expansion of the generation/network, voltage collapse or lost system integrity, excessive equipment damage, replacing damaged equipment (if a spare is available), creating dangers for the public, or creating fires (i.e., dependability takes precedence over security of supply).

Secondly, transmission feeders use duplicate protection systems, and such systems can be distance/distance or current differential/distance. The selection depends basically upon the cost, type, and quality of communications systems available and utility policy. PTT/DCB schemes will generally replace the distance/distance option, to provide the optimum outcome. The option current differential/distance allows the distance system to be either a PTT or DCB scheme, and network or customer factors will generally select the scheme according to the dependability/security requirements for a given case. These factors could include the following:

- Increased security of supply through single-pole tripping and fast autoreclose (where suitable):
  - About 80 percent of feeder faults are transient earth faults for which clearing occurs by single-pole tripping and fast autoreclose (a blocking scheme may be better).
  - The stability of the power system: If the stability of a power system depends on all faults being cleared in a time shorter than the Zone 2 time delay (typically 400 ms), then a blocking scheme may be better (see Appendix 9: Present Environment and Digital Communications) because any loss in the communications channel will not negatively impact the critical performance of the protection scheme. A similar argument applies to interconnecting feeders or very long feeders and possible voltage collapse.
  - Varying short-circuit levels: If it is possible for one feeder terminal to become weak (a strong source is disconnected, for example), and the feeder tripping time should not be compromised, then a blocking scheme becomes advantageous. If a fault were to occur in front of the weak terminal and the fault current were so low that it could not pick up the fault detectors, the weak terminal may not detect this fault. If a permissive scheme were used, the weak terminal would not send a signal to the strong terminal, and tripping would be delayed. This would not be the case for a blocking scheme, because the strong terminal would trip only after a short delay (typically 40 ms). Blocking for an external fault is not an issue in this case, because the strong terminal will provide enough current through the relay at the weak terminal that the scheme will detect the fault and send the appropriate blocking signal.
  - Network configuration: If a new feeder is built parallel to an existing feeder, it is common practice for parallel feeders to share a common protection philosophy.
  - Generator/load security requirements: The customer may be ready to procure power at different levels of supply security, and this may influence the selection. However, clearance of all faults is still necessary. It is not uncommon in such cases to use duplicate DCB schemes.
  - Available communications infrastructure: Protection and communication parts are intertangled and must be considered concurrently when designing a protection scheme based upon the previously listed basic factors. The cost of a communications system can be many times the protection system cost; so typically protection ‘accommodates,’ unless network conditions or customer requirements overrule cost.

Usually the first system is easy (PLC or OPGW); the second independent system is more difficult in terms of

obtaining agreement and cost. Added to this is the multifunctionality of numerical protection relays. Essentially, protection engineers determine the appropriate teleprotection schemes and their communications requirements. The communications engineer must then balance the merits of each communications system against what a project's acceptable maximum costs allow or the expense a customer dictates. Obtaining agreement can be difficult. For the case of a second system on a 132 kV radial feeder, the agreed outcome was for Zone 2 distance protection at a utility source where Zone 2 overreached into the customer's plant and could trip after six cycles. This was acceptable for the feeder rating and stability, and it met the customer and connection agreement.

## X. APPENDIX 3: COORDINATION OF OPERATING PRINCIPLES

Modern protection engineers do not often have the luxury of selecting the protective relays at both ends of a feeder terminal. It is probable that the relays at either end come from different manufacturers or technology eras. To coordinate these relays with each other properly in a DCB scheme, engineers must understand thoroughly the operating principle for each relay.

### A. Distance elements

Distance is the most common fault detection function in communications-assisted schemes, so understanding how distance elements operate is key to understanding how a scheme will function under different operating conditions. When referring to a distance element, we refer not only to the distance calculation but to all other supervisory conditions that make up the element. Fig. 24 is a simple distance element sketch.

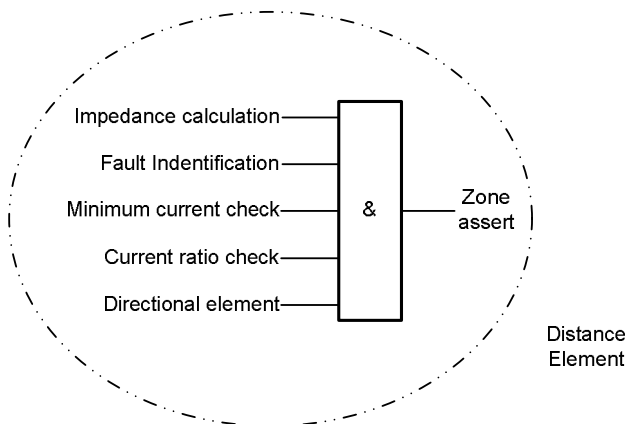


Fig. 24. Sketch of a simple numerical distance element

Listed are the typical distance element main components.

- Mho Distance Comparator
 

The difference between mho elements of different make and model is primarily in the type of polarizing voltage. Older generation relays (electromechanical and even discrete component relays) are either self polarized or cross polarized. Modern relays (numerical relays) add a memory voltage component to their polarizing voltages.

- Self polarization—Relays with this type of voltage polarization, have no mho expansion, and the relay cannot determine directionality for faults close to the terminal (voltage  $\approx 0$ ).
- Cross polarization—A relay with this type of voltage polarization has mho expansion [4] and can determine directionality for phase-to ground and phase-to-phase faults close to the terminal. It cannot determine directionality for three-phase faults close to the terminal.
- Memory polarized—Relays with this type of voltage have mho expansion and can determine directionality for all fault types close to the terminal. Keeping a fully static voltage for polarization can jeopardize the element's performance if the system swings. In such a situation, the memory needs to expire, and the element should switch to a self-polarized or cross-polarized mode. It is also possible to have a mixed mode polarization in which, for example, a positive-sequence voltage (a form of cross-polarization) combines with a memorized portion of the positive-sequence voltage, and the memory decays over time after triggering for a fault.

Although these are all mho distance elements, they do not operate in the same manner. Let us examine how these differences impact the performance of a DCB scheme.

Assume that the relays at either end of the feeder are self polarized and that the fault is close behind the local relay (external to the feeder). The remote relay will detect this fault easily, but the local relay cannot detect the fault behind it because the voltage is too low. The result is that the remote relay trips for a fault outside the feeder. The same will happen if we use two cross-polarized relays, and the fault happens to be a three-phase fault.

Consider the case where we use two relays with memory voltage but with different time constants. For a three-phase fault behind the relay with the shorter time constant, the relay may stop sending a blocking signal when its memory voltage decays past a certain point. If the fault were still present, the remote relay would trip because it either did not receive a blocking signal, or the blocking signal dropped out.

- Quadrilateral Distance Element
  - The main difference between a mho and quadrilateral distance element is that voltage polarizes the mho, whereas current polarizes the quadrilateral element.
  - We do not address the different methods of polarizing the quadrilateral element here, because this element does not impact DCB scheme security significantly; the current at both line ends is approximately the same for external faults. What concerns us primarily here is the construction of the quadrilateral and how it differs from a mho, because a mho element often has to interact and coordinate with a quadrilateral element.

- In a quadrilateral element, you can set the resistive reach independently from the reactance reach, meaning that you can get greater resistive reach from a quadrilateral reach. Because current polarizes the quadrilateral element, it will produce an output for the entire fault duration (Remember that this is not true for a mho element for close-in three-phase faults). Fig. 25 is a plot of the remote relay with a quadrilateral set characteristic, as compared to a mho characteristic of the local relay.

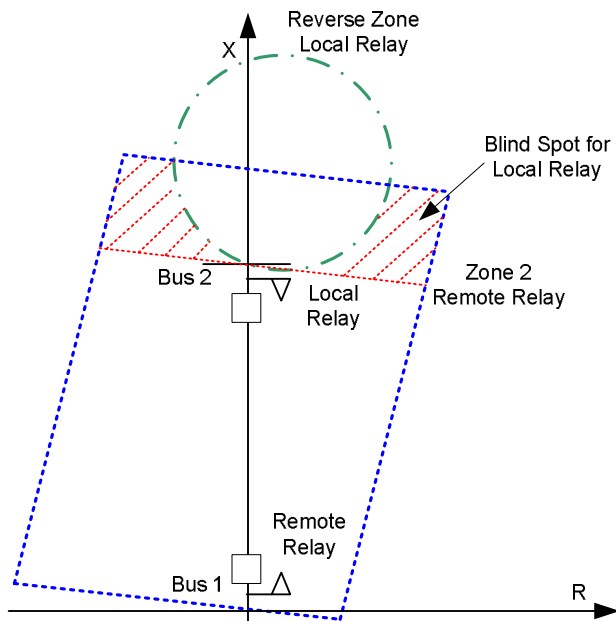


Fig. 25. A simple sketch showing a Quadrilateral distance element and a Mho distance element being used in a DCB scheme

The red area in Fig. 25 is a blind spot for the reverse-looking Z3. This is an overtripping area for the DCB scheme, an area where the remote relay will trip for a fault that the local relay cannot detect (and for which it fails to send a blocking signal). Take this into account when setting the resistive reach of the Zone 2 element.

### B. Fault Identification Logic

Mho or quadrilateral distance elements (the distance calculations) may not be very discriminative in selecting the faulted phase or phases when earth is involved. When earth is not involved the distance element with the lowest calculated impedance is usually the faulted loop.

Therefore, it is possible to use faulted phase identification logic to prevent the earth distance element of the leading phase during a phase-to-phase-to-earth fault from overreaching. This logic differs among manufacturers but, because phase quantities themselves do not provide a reliable output, it often uses sequence quantities. If the logic uses sequence quantities, these quantities must often exceed a certain magnitude to enable the fault identification logic.

For example, one manufacturer uses the angle between the zero-sequence and negative-sequence currents to identify the faulted phase. To enable the logic, the following must be true:

- The magnitude of both the negative-sequence and zero-sequence currents must exceed a user-settable minimum threshold.
- The ratio of the negative-sequence and zero-sequence currents must exceed a fixed minimum value.
- The ratio of the zero-sequence to positive-sequence currents must exceed a fixed threshold.

Fig. 26 is a sketch of the conceptual fault identification logic.

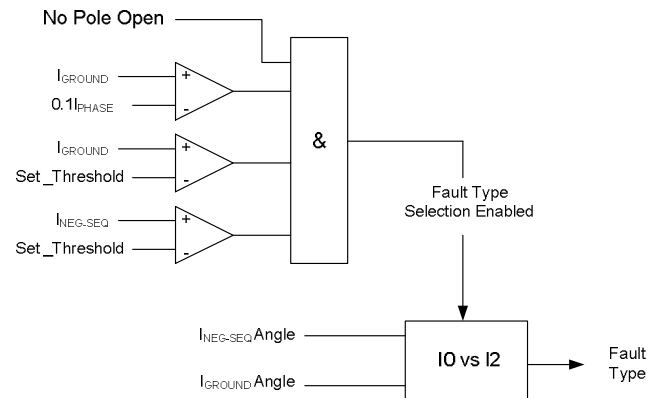


Fig. 26. Conceptual fault identification logic

One of the field cases we described resulted in a misoperation of the DCB scheme because one relay had negative-sequence and zero-sequence minimum pickup thresholds set higher than the other end. As a result, the remote relay picked up for an external fault (Z2), while the overcurrent check in the fault identification logic inhibited the local relay (Z3).

### C. Minimum current checks

For added security, distance elements have a minimum phase current threshold; earth distance elements have an additional zero-sequence or residual current minimum current check. In a two-terminal application, ensure that both ends are set to the same value for a multiterminal application, and that all ends are coordinated so that a reverse-reaching zone at each terminal detects all faults that any of the forward elements at the remote ends detect.

### D. Current ratio checks

Feeders are not always transposed perfectly, so when a three-phase fault occurs on the system, negative-sequence and zero-sequence currents can also flow with the positive-sequence current because of the nontransposition of the phase conductors. The same occurs if a three phase fault occurs on a power system, and one of the current transformers saturates. The relay will measure erroneous negative-sequence and zero-sequence currents. To block earth elements from asserting incorrectly under these conditions, some relays have a negative-sequence to positive-sequence or zero-sequence to negative-sequence current ratio check.

Be careful when setting this value; a value too low could result in the earth element asserting when it should not. Too high a value could result in the earth element not detecting a

fault with a moderate fault resistance. A typical settings value for the I2/I1 ratio or I0/I1 ratio would be about 10 percent.

Using a portion of the positive-sequence current to restrain makes the element respond to the load and can impact sensitivity in multiterminal applications. The amount of restraint depends on the load flow; various terminals can have different degrees of restraint for a given external fault. Typically, it is good practice to reduce the amount of positive-sequence restraint for the blocking elements. This will not impact dependability, because directional comparators will prevent the blocking elements from asserting for forward faults.

#### E. Directional Element Supervision

For added security, schemes can use directional elements to supervise the distance element. DCB teleprotection schemes usually employ directional elements to detect high resistance faults in feeders; we discuss these issues in Section VI. Enhancements to DCB Schemes.

#### F. Directional Elements

To detect high resistance faults reliably within a feeder, protection engineers make use of directional overcurrent elements such as negative-sequence elements or earth elements in addition to distance elements. The teleprotection scheme includes these elements to accelerate the tripping of the feeder in cases of a high resistance fault. These directional elements provide greater sensitivity for the detection of internal faults, but they also considerably increase the effective reach of the relay. Think of a directional element as a distance element with its reach set to infinity (see Fig. 27).

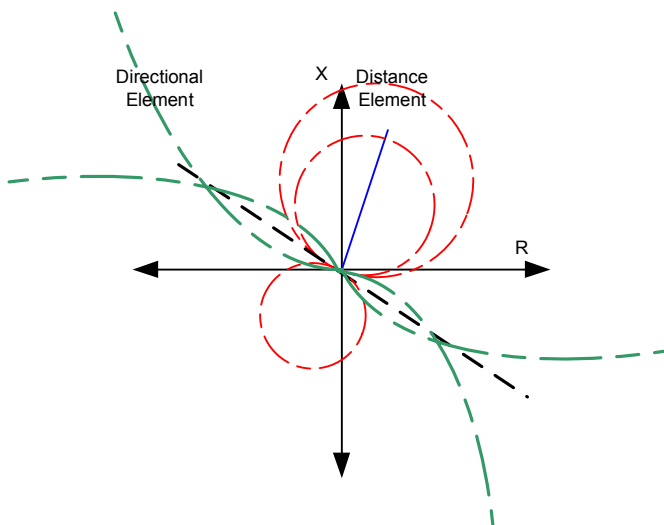


Fig. 27. Plot of distance elements versus a directional element

It is not uncommon for directional elements to detect faults in feeders several buses away. Protection engineers must therefore ensure that the blocking element also detects these faults. Otherwise, the inclusion of these elements in the teleprotection scheme could lead to an unwanted trip of the unfaulted feeder that is contributing part of the fault current.

A further issue when parallel lines are concerned is current reversal. Examine the simple sketches in Fig. 29 a and b.

Assume that both lines are in service and that a fault occurs on Feeder 1 close to Bus B. Assume that the current distribution is as shown in Fig. 29 a, where both feeders contribute to the fault. For the relay  $R_{B2}$  at Bus B, the fault is clearly in the reverse direction. This relay will send a blocking signal to relay  $R_{A2}$ , while the unfaulted line relay remains stable. Relay  $R_{B1}$  will trip its breaker instantaneously, because the fault is in its Zone 1. When the breaker associated with relay  $R_{B1}$  opens, the current through Feeder 2 reverses direction. When this occurs, relay  $R_{B2}$  detects the fault in the forward direction. If at this point relay  $R_{A2}$  is slow to detect the fault in its reverse zone (Zone 3), and we also add in the time delay of the communications channel, relay  $R_{B2}$  can trip incorrectly as a result of the current reversal.

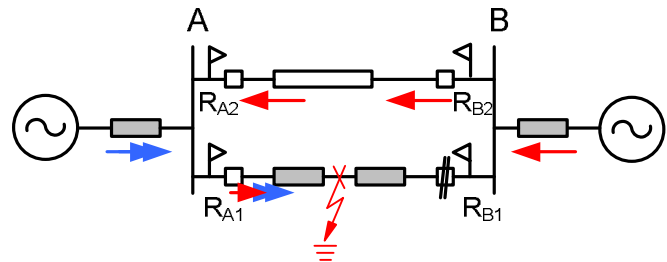


Fig. 28. A simple sketch of a system prone to current reversal

Therefore, to prevent relays from misoperating for the current reversal conditions, the DCB scheme has a delay on the Zone 3 element dropout timer. This ensures blocking of the Zone 2 element in accelerated mode if the relay had a Zone 2 element asserted before the Zone 3 element asserted.

#### G. Processing Interval

This applies only to numerical protection relays. Unlike analog relays, which process the signal continuously, numerical relays process information in discrete time intervals. The type/generation microprocessor in a numerical relay usually determines the processing time interval (processing rate) of the algorithm. Older generation relays processed information generally at a slower rate (four to eight times per power system cycle); new relays process at a rate of eight to 32 times per power system cycle. What this means is that new generation relays can detect a fault more rapidly than older generation relays. Take this into consideration when coordinating these relays in a DCB teleprotection scheme.

The worst case assumes that the tripping relay aligns its processing moments with respect to the fault in such a way that it asserts without consideration of the impact of its processing interval. At the same time, the blocking relay aligns its processing moments in such a way that it misses one processing interval on its way to assert and send the block. As a result, the scheme can add an extra margin equal to the processing interval of the remote relay. This margin comes into play upon use of user-programmable logic at the blocking relay – the protection elements themselves have the processing time blended into their published operating time curves.

In addition, new relays can use fast algorithms such as high speed elements (see Appendix 5: Distance Relay Technology Characteristics).

## XI. APPENDIX 4: DESIGN CRITERIA FOR DCB SCHEME

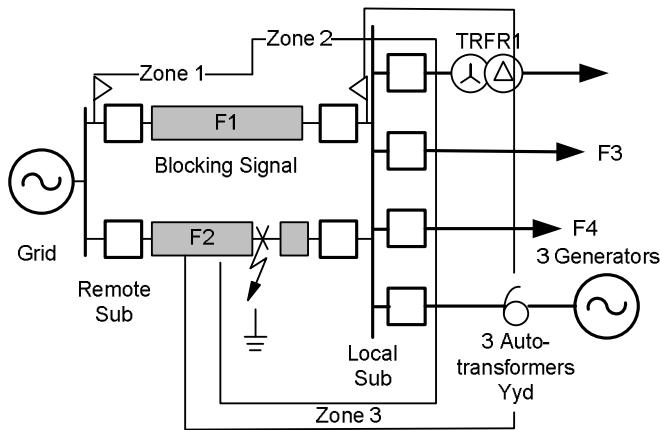


Fig. 29. Allocation of distance zones for DCB scheme on Feeder 1

### A. Scheme Design

We install a distance relay at each end of the feeder, and the settings reflect the local electrical conditions together with coordination with the remote relay. Each distance relay provides three zones of protection as follows:

- Zone 1, which operates instantaneously, is forward looking and set to about 80 percent of feeder impedance. By using this 80 percent setting, we avoid overreaching the remote substation's relaying point because of various error sources. [5] Zone 2 is forward looking. Because Zone 2 is an overreaching zone that we typically set at approximately 120 percent of the feeder's impedance. Distance tripping by Zone 2 is delayed so as to provide coordination with downstream feeders. Typically, we set the Zone 2 time delay at approximately 20 cycles (400 ms on a 50 Hz system). We use this feature primarily to clear remote faults or in a step distance application. When we use this feature in a DCB scheme, a coordination timer delays tripping by means of the Zone 2 element. We set this coordination timer setting at approximately two cycles (40 ms on a 50 Hz system). Many factors determine this time-delayed setting. The dominant factor is the communications delay. Zone 3, which operates instantaneously, is set to detect faults in its reverse direction and to overlap the remote relay's Zone 2 under all conditions. The expectation (for the same relay type) is that the local relay will operate faster than the remote relay because the restraining fault voltage is lower. However, as we discussed previously, we must verify this expectation.

### B. Scheme Operation

There are three scheme operating modes:

- **Fault 1:** For internal feeder faults, for which each relay's Zone 1 operates, the instantaneous tripping occurs well before Zone 2 can trip. No signaling is necessary.
- **Fault 2:** For internal end zone feeder faults, no signaling is necessary – the remote relay's Zone 2

tripping waits briefly (approximately two cycles or 40 ms at 50 Hz, depending on communications delay, etc.) for a blocking signal and then trips. The local relay trips in Zone 1.

- **Fault 3:** For faults external to the feeder, a blocking signal is necessary to stop the remote relay's Zone 2 tripping, and this signal arrives within the waiting time. If the fault persists, Zone 2 trips in backup time. Note, as Fig. 29. illustrates, that Zone 2 sees partially into the transformers, into the parallel feeder, and into the feeders F3 and F4.

### C. Communications requirements

Any of the communications carriers of PLC, microwave, OPGW, radio, or pilot wires are suitable for DCB. The criteria are as follows:

- The signal propagation in the communications system must be fast enough to satisfy the fault clearance time for the protection scheme at the particular electrical location.
- A system should provide a degree of continuous self-monitoring and should be capable, if necessary, of deasserting a failed GUARD signal. The number of repeaters is minimized, and the system should preferably share the same route (see the following text) for one signal.
- The reliability of the system should be equivalent to that of protection equipment.

An interesting quandary in the design process is that protection requirements initially determine the options for the communications systems. The cost and practicality of providing duplicate, independent communications systems impact protection preferences. This is evident where OPGW is used for one protection scheme and the cheapest independent option could be any of the following:

- Microwave, radio, or pilot wires for short distances;
- Microwave (with repeaters), PLC for long distances;
- A second OPGW route. For transmission voltages, this is viable because such schemes typically use two earth wires to achieve the feeder's shielding factor. However, a backup protection strategy should be provided if the communications system(s) fails;
- A nondirect route through various communications systems that satisfies the signal propagation, independence, and reliability requirements. This may be practical because many utilities have meshed communications networks with the capability for signal failover (in 1+1 redundant systems—see Appendix 9: Present Environment and Digital Communications) or rerouting.

### D. Setting Considerations

The setting criteria for this scheme could be as follows:

- Zones 1/2 settings are determined by the following:
  - Need to detect line end open (LEO) faults within the intended reach, including arc resistance cases;

- Need to detect line end closed (LEC) faults within the intended reach and with best coverage for arc resistance;
- A margin of safety (20 percent) to cover error sources, mutual coupling, instrument transformer transient behavior (such as a CCVT transient), relay inaccuracies;
- Need to ensure that Zone 2 does not trip before any external, slower protection schemes. For 275 kV lines, a time of 400 ms is generally necessary to time grade over a remote substation's CB fail protection (two cycle CBs); Zone 2 blocking time delay is set according to relays' operating time difference, communications time delay, output and input relay delays, safety time margin, or to achieve maximum permissible fault clearing time (See Section IV. Sample Field Cases).

Thus, it is possible to set the Zone 2 reach at 150 percent of the feeder.

- Zone 3 settings could be determined by the following:
  - Need to overlap the remote relay's Zone 2 reach past the relaying point ( i.e., remote relay's Zone 2 reach – line impedance);
  - Need to detect all faults that the remote Zone 2 relay can detect.
  - Need to provide adequate coverage for arc resistance (including for the remote relay's Zone 2 to ensure that it does not operate on load encroachment or have load dependence);
  - Need for a margin of dependability (10 to 20 percent) to cover error sources and relay inaccuracies.
- In general, we should set Z3 according to both remote Z2 settings and system conditions. For example, a Z3 overcurrent supervision threshold (with a margin) should be less than an overcurrent supervision level at the remote Z2. Setting both thresholds independently according to the system short circuit level can cause problems when the short circuit data are inaccurate or when the system has evolved since calculation of the original settings.
- Supervision elements are relay specific. However, as we have stated, it is critical for the local relay to operate for faults external to the feeder but visible to the remote relay. We must also consider the conditions of a healthy feeder during an external fault. Some general guidelines are as follows:
  - Phase faults:
 

Set forward supervision elements in excess of load current but at approximately 70 percent of minimum fault current for remote three-phase faults or two-phase faults that the relay must detect. Note that for end zone faults less than load current, it will be necessary to set elements to less than load current.

Set reverse supervision elements at approximately 60 percent of the remote relay's forward threshold;

Often, schemes use negative-sequence directional elements because of their greater sensitivity in detecting higher resistance faults. You must ensure, however, that the pickup settings for these elements are coordinated. Note that if this element is set to be very sensitive, it will pick up for any system unbalance, whether it is an unbalanced load condition, or an open breaker farther down the system, etc. This is generally not a problem because negative-sequence current entering the feeder will also exit the feeder. Negative-sequence charging current can generally be disregarded. However, it is good practice to avoid setting this element too sensitive and to time delay it by a cycle or two. This is because the element can assert when you have a load change. Ensure that if you are going to apply negative-sequence current at the local terminal, you also apply it at the remote terminal and verify that the two elements have the same pickup threshold.

- Earth faults:

The first thing to remember is that this element was not designed to detect extremely high resistance earth faults. Also remember that a nontransposed feeder under normal operating conditions will draw a residual current because of unbalance. In general, set the earth current element pickup at about 10 percent of the nominal CT secondary current. This should be about the limit of the earth faults the relay should need to detect. If you want to detect lower current earth faults, study this issue carefully and remember to take into account factors such as lack of or poor line transposition, normal load unbalance, and current transformer error (remember that the earth current is the sum of the three-phase currents, and an error in one of the phase CTs will carry through to the earth current calculation). A setting of 10 percent prevents the element from asserting for normal load conditions and prevents the element from operating if you have a heavy three-phase through fault and one of the phase CTs saturates. Again, it is best that this element be time delayed slightly for extra security.

#### *E. For Overcurrent and Earth Elements*

Set forward supervision elements at approximately 70 percent of minimum fault current for remote faults the relay must detect.

Set reverse supervision elements at approximately 60 percent of the remote relay's forward threshold.

For very long lines (large charging current) and high sensitivity requirements, consider the impact of the charging current on the blocking function under external faults.

### F. Out-of-Step Blocking (Power Swing Blocking)

In the electricity network, it is possible to lose synchronism between generator areas or interconnected systems, most probably as the result of a severe fault and significant delay in clearing this fault. Thus, a (damped) oscillation exists between the generators through inertie feeders. Distance relays can detect the angular difference of this three-phase oscillation as a low varying impedance encroaching on or passing through their zones.

To prevent the system from separating at this critical time, relays can be set with out-of-step detection logic. This logic blocks the distance elements (Zone 1, Zone 2, and Zone 3, etc.) from asserting their outputs. So, if OOS is enabled, ensure that it is set in both relays. Also verify that, when an OOS condition blocks the remote relay's Zone 3 element, an OOS element also blocks the local relay's Zone 2 element.

### G. Load Encroachment

For long, heavily loaded lines, it is often difficult (if not impossible) to both provide protection for the feeder and allow maximum power transfer. To prevent the distance element from operating in the heavy load region, we use load encroachment. Load encroachment blocks the distance element if the positive-sequence impedance is within the load region. Again, ensure that if you use load encroachment, you set it in both relays and coordinate the settings. Because Zone 3 is generally not easily asserted as a result of load, this may be a mute point. However, if the scheme asserts load encroachment, ensure that the local relay's Zone 2 cannot at any time assert as a result of load and that the remote relay Zone 3 element is blocked because of load encroachment.

## XII. APPENDIX 5: DISTANCE RELAY TECHNOLOGY CHARACTERISTICS

The successful application and operation of distance teleprotection schemes requires a good understanding of distance relaying, relay technology characteristics, and the specific characteristics of each relay in the scheme. This is critical when a relay of different technology replaces a relay in a scheme, such as in Fig. 32.



Fig. 30. First generation (electromechanical) protection relay



Fig. 31. Second generation (solid state) protection relay



Fig. 32. Third generation (numerical) protection relay.

### A. Analog Technology

Analog relays used electromechanical devices such as induction cup comparators for distance elements. Generally, for these relays, the following were true:

- The distance characteristic was purchased as either mho or quadrilateral. Manufacturers specialized in one shape. Typical accuracies at set line angle were Zone 1:  $\pm 5\%$ , Zone 2:  $\pm 10\%$ , Zone 3:  $\pm 10\%$  (if purchased), starting zone (non directional fault detection element):  $\pm 15\%$ .
- They operated at about 1.25–2.5 cycles for a complete set of distance elements (full) or at about 1.75–3.25 cycles for a switched relay where the fault type switched the appropriate V and I to the single distance element. In addition, the speed of pickup was fastest at the origin, reasonably flat for 20–60% of reach and increasingly slower at greater than about 60 percent;
- Self-polarizing, cross-polarizing, or relatively crude memory voltages maintained directionality for close-in faults (off set characteristic). These could be compromised under some fault conditions.
- They used composite distance elements that were found to be compromised under some fault conditions. For example, one particular relay used a voltage-modified overcurrent element.
- Sophisticated fault identification logic was not included. Close-in faults with very high currents could cause nonfaulted phase elements to operate (a B-phase earth fault, for example, could operate the A-B and B-C elements). Prevention of such misoperations required careful application;
- Faulted phase indication was unreliable.

### B. Solid-State Technology

Solid-state relays used solid-state comparators or simple (4 bit) microprocessors for processing the output of the distance algorithm. Generally, the following was true for these relays:

- The distance characteristic was purchased as mho, quadrilateral, or an option. Manufacturers provided special characteristics for Zone 3 to cater for load encroachment (e.g., lens, tomato). Typical accuracies at set line angle were Zones 1–2:  $\pm 5\%$ , Zone 3:  $\pm 10\%$  (if available).
- The relays operated at about 1.25–2.5 cycles for a complete set of distance elements; speed of operation over the reach was slightly flatter.
- Cross polarization or (improved) memory voltages maintained directionality for close-in faults (offset characteristic). These were better but could still be compromised under some fault conditions.
- Faulted phase indication reliability improved.

### C. Numerical Technology

Numerical relays use microprocessors and electrical theory-based algorithms for distance elements. First generation relays had conventional distance elements, while second generation relays use a high-speed distance algorithm based upon the Superposition Theorem[7]. Generally, for these relays, the following are true:

- The distance characteristic is settable as mho, quadrilateral, or both. Some manufacturers provide special polygon characteristic. Typical accuracies at set line angle are Zones 1-3:  $\pm 5\%$ , Zones 4–5:  $\pm 10\%$  (if available) .
- These relays operate at about 1.0–1.75 cycles for conventional distance elements. The speed of pickup is comparably flatter over the reach.
- These relays operate at about 0.6–1.25 cycles for the delta algorithm. The speed of pickup is comparably flatter over the reach, where the delta elements operate. It is critical to know for these relays which zones have the delta algorithm, reach of the relays within the zone of protection (e.g., 75% conventional reach), and whether the algorithm is disabled after fault detection, (e.g., two cycles).
- They provide reliable faulted phase identification, especially for close-in faults with high currents.
- Good memory voltages maintain directionality for close-in faults (offset characteristic). This is evident in superior performance over the system impedance ratio (SIR—source impedance/set relay impedance), which indicates the amount of fault voltage (high SIR = low fault voltage).

- Supervision elements improve relay performance (for close-in faults, for example) and dependability. However, these elements must be applied carefully so that they are not compromised under some fault conditions.
- These relays provide comprehensive logic, as well as event and disturbance recording.

The following figures present examples of these characteristics (see also Fig. 25).

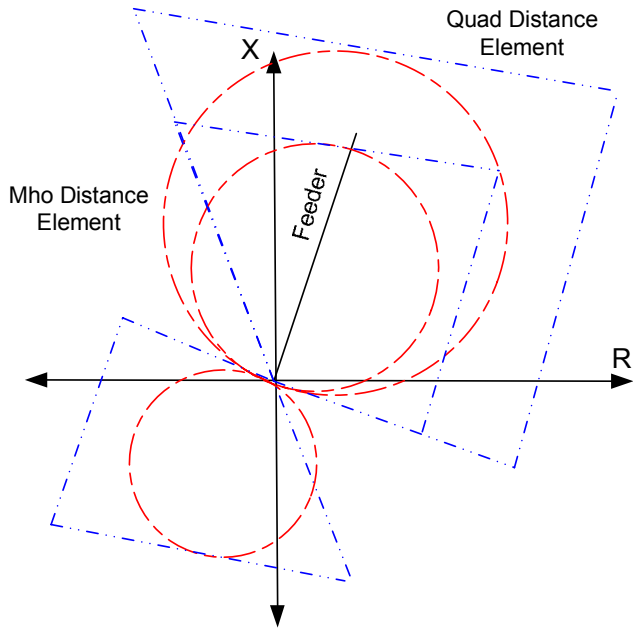


Fig. 33. Plots of mho and quadrilateral distance element characteristics

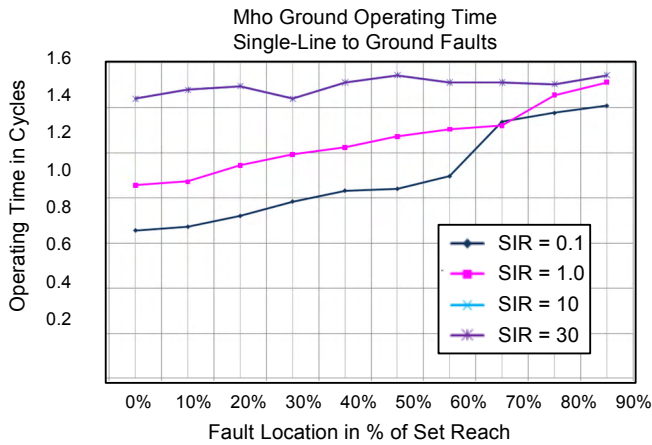


Fig. 34. Performance of a conventional mho ground distance element

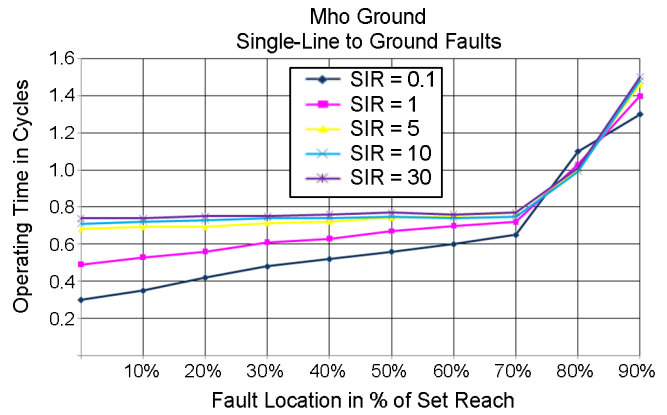


Fig. 35. Performance of a delta mho ground distance element over SIR range 0.1 to 30 (Note: reach is limited to 70%)

### XIII. APPENDIX 6: TROUBLESHOOTING FIELD CASES

#### A. Introduction

A recent investigation into the incorrect tripping of a healthy feeder that used a DCB scheme was severely constrained because the local relay was not set to record the blocking event. This section explains how investigators examined this misoperation and how they recreated missing data was from various sources, converted these data into COMTRADE format, and replayed the data into the protection relay to confirm their findings.

#### B. Investigation Process

##### 1) Step 1: Collection and Validation of Data

We must determine the feeders' operating configurations, the availability of records, relay settings, setting calculations and recent test results, and the exact details of the fault and physical location. These records must be quickly sourced (in an unfiltered, high sampling rate) for the faulted feeder and all contributing feeders so that subsequent events do not overwrite them. The setting files are sourced from the relevant protection relays; these files are not copies stored in a central depository.

In addition, we must take into account that data in the substations' SCADA system is frequently of suspect quality. This is because of the following:

- Small time differences in various equipment when a time accuracy of 2 ms or less is necessary. Thus it important to appreciate the quality of time synchronization available in substation equipment and between substations with different technologies;
- The RTU may overload its buffer during a major event and cause erratic SCADA recording;
- Alarms may be sourced from slave relays that can add 10 to 20 ms to the genuine signal/trip time;
- The debounce time delay (1–5 ms) may be added to the true signal receive time, or the time is not recorded to the nearest ms;

- An absolute time reference was not connected, or the date was not set in the equipment;
- Inconsistent naming of alarms between relays, RTUs, and possibly between substations. This causes confusion and requires validation of alarm labeling.

Thankfully it is usually possible to use fault inception as a synchronizing instant for all records. For earth faults, we should use residual current; for two-phase faults, they should use negative-sequence current. Thus, the disturbance records of protection relays show the fault inception and their respective output signals, which we can then relate to SCADA alarm records.

The first task involves collecting all available data, sorting and validating data for time and labeling quality, and notating areas of missing or suspect data. We should then determine the pickup and drop off events for all protection relays and CB tripping. Step 1 is critical to the process. It provides us a very valuable understanding of the total event and the ability to postulate possible failure theories.

2) Step 2: Create Time Line Diagrams

We use the validated data to create time-line diagrams for faulted and healthy feeders in either linear or tabular form and color code common events or missing critical data. Table IV shows an example. This format enables a good visualization of events, their relationship to expected behaviors (pickups/dropouts), and additional validation of data quality.

The example shows the following:

- The protection systems for the faulted feeder tripped the feeder correctly;
- Transmission of the blocking signal from the healthy DCB scheme occurred too late, and the pattern of resetting possibly indicates marginal sensitivity;
- A communications delay of 20 ms is ok;
- The F1 relay fast fault detection of an external fault possibly indicates a mismatch in operating speed (possibly resulting from delta distance elements, for example).

TABLE IV  
TIME LINE DATA (50 HZ NETWORK)

Event 1: 2/1/09 13:25:34					
Faulted Feeder 2			Healthy Feeder 1		
Remote Sub 1	ms	Local Sub	Remote Sub 2	ms	Local Sub
	552	Fault starts		552	Fault starts
			DZ 2 detected	563	
	567	DZ trip Z1			
DZ 2 detected	568				
I Diff X trip	573				
	577	I Diff X trip			
				581	Blk Send

Event 1: 2/1/09 13:25:34					
Faulted Feeder 2			Healthy Feeder 1		
Remote Sub 1	ms	Local Sub	Remote Sub 2	ms	Local Sub
				589	Blk reset
	597	CB open	DZ 2 fast trip	596	
CB open	603		Blk Rec	601	Blk Send
	607	DZ Z1 reset		606	Blk reset
DZ 2 reset	608	I Diff X reset	Blk reset	609	
I Diff X reset	613				
			Blk Rec	616	
			Blk reset	620	
			CB open	630	
			DZ 2 reset	640	
Fault duration 51 ms		Fault duration 45 ms	Fault duration 78 ms		

3) Step 3: Data Analysis

Now we have the “jig saw” pieces laid out ready to piece together into little groups and then bigger groups. The following points should be helpful:

- Ignoring what happened, write down your expectations of what would happen and where and when you expected these events to occur (i.e., the big picture). Keep this firmly in your mind as you analyze each data piece from time zero;
- Check that the prefault load conditions were correct. Possible problems here could include use of incorrect records, reversed polarity, or even swapped phases. This is more probable in a bus differential scheme, where load current does not produce enough spill current to cause a trip;
- Analyze by validating actual data against the big picture, looking for patterns or unusual events, lateral thinking, suspecting data (e.g., errors in time stamping, incorrect CT ratio or polarity, etc.). Such analysis is a developed art!
- Identify root causes or salient events (a missing action, for example) so as to postulate a theory. If no such causes are evident, discuss findings with protection field staff and have a colleague review and ask searching questions of all data with you (two heads are better than one).
- Assume that nothing is correct, especially the commissioning process. Always independently validate data/results/findings.
- Comment: For Field Case 1, at this step there was no theory why the blocking relay did not send a blocking signal. The external feeder fault was clearly within the set and calculated reaches, and the negative-sequence current exceeded pickup values. Examination of the

relay logic diagrams did not show enough detail to identify a cause.

#### 4) Step 4: Postulate a Theory

Assuming that you postulated a theory, perform the following actions:

- Devise a plan to validate your theory—usually this plan involves testing with representative quantities.
- If satisfied with your theory, formulate corrective actions and discuss these actions with the relay manufacturer (where appropriate);

Assuming that you were unable to postulate a theory, refer the event to the relay manufacturer with information obtained from performing the following. It is critical that utility based information be presented to the relay manufacturer in an easily understood manner (a relay manufacturer, for example, should not have to scan the terse labeling of a SCADA printout).

- Answer whether misoperations caused a trip and loss of supply. The answer to this question determines the speed of the response;
- Obtain relay(s) ID, firmware number, and setting file(s);
- Obtain all relevant information from Step 2 plus the local network diagram;
- Obtain contact details for the utility's expert to discuss the event, request more details, and discuss findings;
- Request the name of a relay manufacturer contact and establish a date by which the manufacturer should respond.

Usually, the relay manufacturer will provide a theory, explanation, or solution, but it is also possible for both parties to develop a joint solution. It is important, in any case, that there be a good working relationship between parties.

There are three reasons for referring the event to the manufacturer:

1. To obtain the benefit of the manufacturer's collective knowledge and experience of the product's operation;
2. To obtain revelation of undocumented features or characteristics. The utility must appreciate that the manufacturer cannot provide 100 percent documentation of the intellectual property that makes their relay operate;
3. If there is no feasible theory talk to the field personal and check to see if a similar event has occurred or if any vital information was not disclosed at this stage it might be feasible to use simulation tools , such as an RTDS to recreate the event and gain better insight.

#### 5) Step 5: Validate Solution or Corrective Action

Validate the solution or corrective actions by testing. It is very important that the utility check the relay manufacturer's response and that utility personnel completely understood the solution. Additional questions may be necessary.

It is important to determine whether corrective actions are relevant to other protection systems. For example, we were able to extrapolate the finding of Field Case 1 for the DCB scheme to a POTT scheme that uses a Zone 3 element (see Appendix 1: Types of Teleprotection Schemes).

#### 6) Step 6: Document

Document the investigation, its findings, and any system deficiencies that needed to be addressed (e.g., appropriate fault recording, testing deficiency). Store the document for reference during the expected life of a scheme.

Ensure that relevant staff members are informed, that they understand the findings, and that there have been appropriate corrective actions. Suitable notation of findings should be incorporated into protection design processes.

### C. Manipulating COMTRADE files

#### 1) Introduction

The COMTRADE standard specifies a common format for transient data exchange.[8] Presently, there are 1991 and 1999 standards, although a new standard is scheduled for publication in 2009. Look in the \*.cfg file to see the year standard. Protection relays may generate disturbance record files for recording the sampled V and I for a trip operation. You can convert such a file to COMTRADE format to replay the recording through RTDS, Omicron™ or Doble™ test equipment into a protection relay.

The presented example created a test file from a local tripped relay (on faulted feeder) and the remote tripped relay (on a healthy feeder) so as to simulate the local blocking relay. The process used the voltage from the local relay (16 samples/cycle) and current from the remote relay (8 samples/cycle) for a 50 Hz system. Only voltages and currents were necessary. Obviously, you would not want to mix filtered and unfiltered files.

#### 2) Manipulating files

The following steps outline the procedure for manipulating files:

1. Ensure that original files contain a common element to synchronize data. For an earth fault, use residual current; for a phase fault, use a negative-sequence current or phase current. Keep these synchronizing data throughout the process and discard this information at the end;
2. If necessary, convert files to COMTRADE format through use of the manufacturer's application program to export the file in COMTRADE ASCII format (see Fig. 36). If this is not available, and the source file is text based, you can perform this conversion in Excel™ with column parsing. However, this method is prone to error;
3. If original files have a different sampling rate, it is necessary to normalize these files to the higher sampling rate. Fig. 37 shows an example. Repeat this step to convert from 1991 to 1999 format;
4. Perform the cut-and-paste process of two files manually, because we cannot trust software to do this exactly right. You should have two sets of COMTRADE files with the same sampling rate and same year standard. Save new files with a different name so as to preserve the original files;
5. Import two .dat files into Excel as two worksheets in column-oriented format with analog data in the same

sequence. Discard any digital signals. Put headings (from .cfg files) on the top row for ease of reference, and highlight the synchronizing data points (fault inception);

6. Save the Local worksheet with a new name;
7. From the Remote file, copy and paste headings, sample numbers, sample time entries, and data values for currents and synchronizing data into adjacent columns of the Local worksheet;
8. Use Excel to move blocks of currents and synchronizing data to align synchronization points (see Fig. 38);
9. Tidy up the data file and DELETE excess data such as headings, synchronizing data, and excess sample numbers.
10. To increase pre-fault data, find repetitive load data of one cycle and insert and copy these data into a file; renumber samples. (Distance relays require a number of cycles of pre-fault voltage to ensure that their polarizing memory is full.) Ensure that the number of sample rows agrees with the value in the \*.cfg file;
11. Use the **Save As** command to save data files in \*.csv format and with the filename name.dat, which forces correct naming in Excel. Otherwise, the filename becomes name.dat.csv;
12. Create a new configuration file by copying the Local file with a new name (name.cfg) in Notepad™ and opening it. Open a second copy of Notebook and open the Remote \*.cfg file and copy and paste channels into the new file. (Do not use Excel for this task because it deletes null fields.) Add CT and VT ratios and primary data fields to the analog description so that the test set can convert data into secondary values. Ensure use of the same filename \*.dat and \*.cfg files;
13. Test that application software reads the new COMTRADE file (see Fig. 40). If this fails, check the structure of the file in Notepad to ensure that it appears correct;
14. For first replay, check voltage and current values against original values to see that they are correct. The direction of current flow and signal amplitudes can be reversed/changed in the test set.

3) Failure Modes

Should the recreated COMRADE file not produce the results you expect, the following are a few pointers to aid you in troubleshooting the recreated file;

1. Ensure that the first sample starts at 1 and with a time of 0;
2. Ensure that output frequency is nominal (a replay of a processed file caused the relay to misoperate, and a keen observation showed that the test frequency was 40 Hz!);
3. When replaying a file through test equipment into the relay, check that its operation is correct. The data file can have such unwanted features as a current with small voltages that equals tripping by a distance relay.

The first CB pole to open can cause distortion of phase V and I;

4. Replaying a filtered source data test file can cause a relay to respond differently; because this is the same as effectively double filtering the input to the algorithm(s).

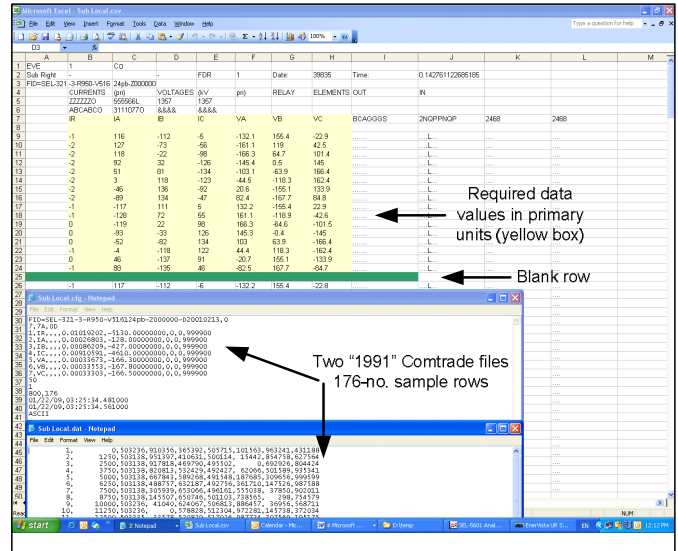


Fig. 36. Example of disturbance record shown in Excel and COMTRADE file set

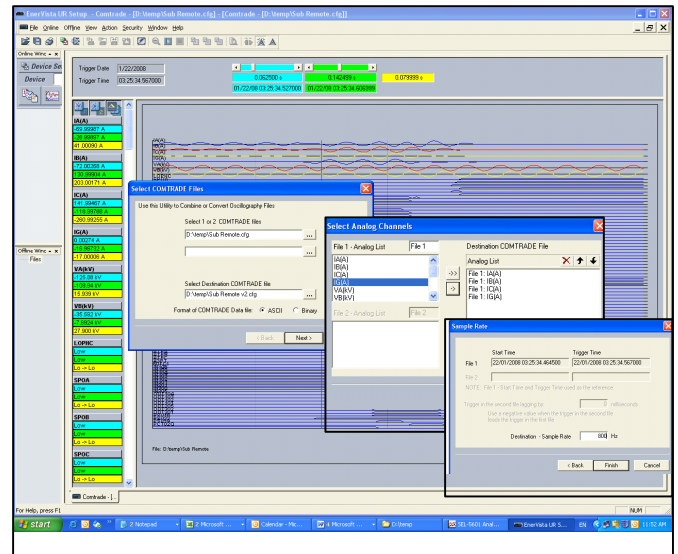


Fig. 37. Converting sample rate process using a available software

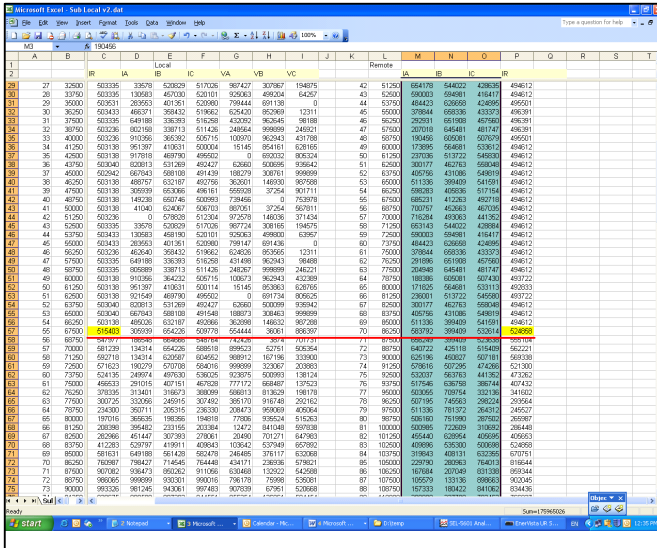


Fig. 38. Example showing synchronization of two data files (yellow boxes and sample row numbers) and remote currents (green boxes) ready to cut and paste over local currents

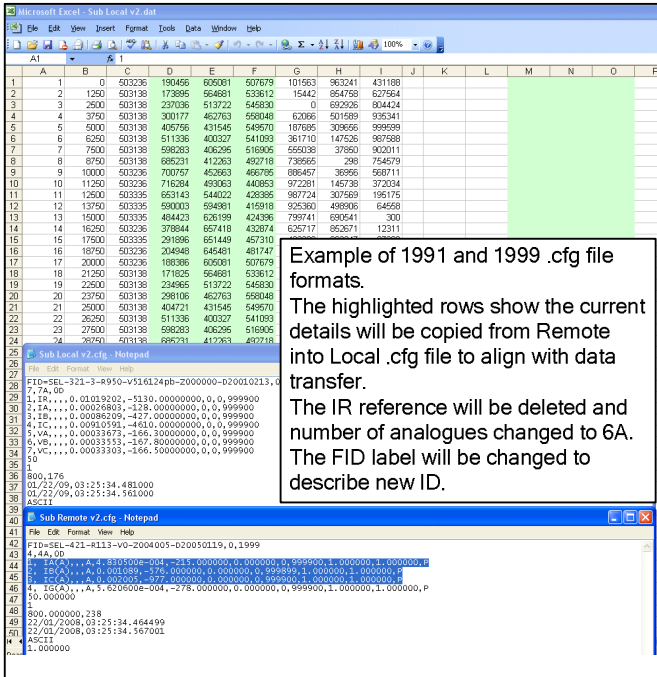


Fig. 39. Example showing current data copied to columns D-F. Columns C and K-P must be deleted to match final format

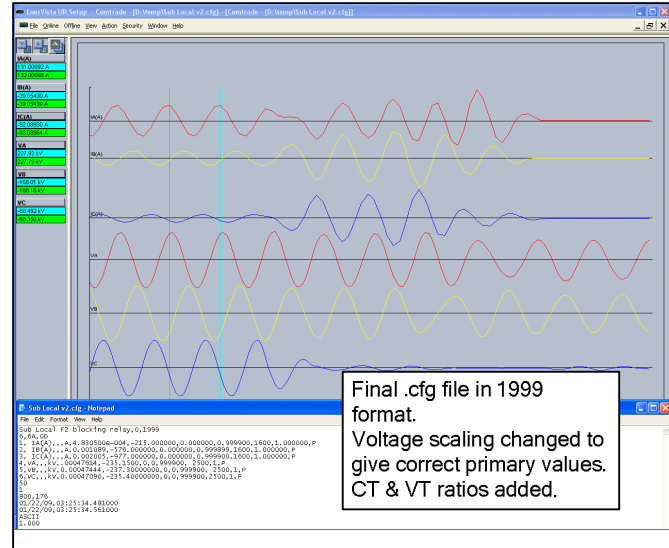


Fig. 40. Final test file was successfully read by COMTRADE reader

XIV. APPENDIX 7: PRINCIPLES OF PROTECTION

Transmission utilities use duplicate protection systems that can consist of different relay hardware and operating principles that operate independently to achieve the highest probability of tripping. This appendix reviews the principles of protection; diversity, redundancy, and independence that have resulted from utility experiences with misoperations.

Utilities use these principles to distribute and minimize the “holes in the proverbial Swiss cheese” to reduce the probability of a resulting major disaster (usually, these holes are unforeseen irregularities such as those we discuss in the following text. From experience in Australia, a major disaster (e.g., transformer on fire, burned out transformer, sequential CB fail event, bent generator shaft, wide-area blackout) occurs about every decade. For 2007 in North America, NERC reports that there were more than 40 protection misoperations that caused bulk power system disturbances [10]. Any actions that can compromise these principles must be very carefully evaluated and proved. As a manager once said, “We use mass production processes to build our substations. We’re very efficient at multiplying our mistake until we find it!”

A. Diversity

Utilities commonly use different operating principles for protection relays so that at least one protection relay will trip under adverse network conditions (network islanding, for example), fault behavior (such as an evolving fault), or irregularity. One of the worst examples of a protection relay misoperating under adverse conditions was a new model numerical distance relay that REBOUT when the feeder fault occurred and failed to trip. The diverse Main 2 distance relay tripped correctly [10]. In addition to ensuring operation of at least one protection relay, utilities design diversity and redundancy into protection schemes to overcome such common mode failures as the following:

- hardware component incompatibility (previous example);
- bug(s) in firmware;

- misunderstanding the content of a relay manual because of ambiguity, language translation, absence of vital information, volume of material, poor referencing, inadequate/poor training, etc.

### B. Redundancy

The level of redundancy depends upon the following:

- Electricity market rules or standards (NERC, for example [11]).
- The utility's protection policy and its confidence in the reliability of relays, their settings, and circuitry;
- The acceptable cost for replicating systems in contrast to common usage or one system. EHV networks use duplicate systems, and UHV networks can use duplicate or triplicate systems. Transmission is a high power network, so any unnecessary supply interruption, voltage disturbance or network instability can result in very high consequential losses for the nation. Therefore, the cost of duplication when amortized over the life of the network, is acceptable and prudent.

We provide many examples in this paper of the need for redundancy.

Redundant systems facilitate maintenance activities. In addition, duplicate protection systems are more dependable, faster, and more secure than single systems that have additional backup distance zones (time graded) to look into the next feeder. Such zones are prone to trip on load encroachment, may not trip because of infeed magnification, and will limit load transfer capability.

### C. Independence

The test for true independence is whether a single component failure event can prevent tripping during a fault or a reclose event, or cause widespread damage/failure to equipment. Historically, true independence started at the CT/VT and ended at separate trip coils on a common CB.

A summary of independent assets:

- The utility duplicated CT and VT secondary windings for each protection function, with the possible exception of CB fail. The number of windings results in incremental cost for the HV insulator and tank components. Separate CT cores result in easy achievement of rating, location, and overlap of protective zones;
- The utility duplicated battery and chargers. Initially, the utility used a single battery bank with segregated fused circuits, but solid state and numerical equipment increased the bank size until the utility decided to split the bank into two independent units. In conjunction with the old battery bank, a number of disastrous events occurred where an open circuit bank prevented tripping and resulted in destruction of a major plant or melting of a feeder's conductors.

It is critical for a more reliable supply that diodes are not connected from each bank to a common point—a forward-biased diode will allow a reverse direction signal to travel

through it, provided that the signal's current is less than the forward current;

- Circuitry and cables and their routing/segregation (to prevent fire damage from, for example, an inadvertent open circuit CT) are independent. Any necessary transfer of signal between circuit systems is galvanically isolated (such as for an armature relay). A separate contact is used for each load instead of one contact with common loads and/or use of diodes. This prevents sneak circuits allowing back feeding of signals with unwanted consequences. LV time signals such as IRIG B should be duplicated and independent, with wiring segregated from secondary circuitry, so that a common failure of both protection schemes cannot occur. This also helps reduce the loading of their drivers;
- Control circuitry is generally allocated to one system to enable simple interconnection;
- Protection relays are independent; the utility must determine the level of integration of functions in one box. Generally, a division upon plant function (transformer, bus coupler, for example) enables good maintenance procedures, isolation practices, and reduced human errors. In addition to the use of numerical relays, a utility can use a common hardware platform and operating system for different protection types. The utility can decide to exclude common hardware platform relays for duplicate protection;
- Teleprotection communications systems are duplicated and independent in equipment. These systems route for entry into the substation and coordinate for insulation rating within the relay panel [13]. However, with suitable designing, it is acceptable for Main 1 and Main 2 teleprotection signals to travel independent channels on each system. Utility personnel must understand and be able to ultimately control by protection practices the capability of digital communications systems to switch or reroute signals. This may become difficult because teleprotection is a low-volume, time-critical user at odds with modern communications processes and design;
- Engineering data communications systems are now connected to protection relays. Failures of RS-232 equipment have caused protection relays to fail (one undetected and one alarmed) because of the relay's microprocessor waiting for the equipment to release its RS-232. There have been no reports, except for spamming, of Ethernet-based failures.

Another problem with this data equipment results from it not being hardened for use in substations. This means that the equipment could become paralyzed, with unwanted impacts upon protection relays. Therefore, the utility should have independent duplicates of this equipment and segregate equipment wiring from secondary circuitry.

Obviously, the relay manufacturer cannot test the impact of all data equipment upon its relay, but it can provide alarms, design the relay communications port or microprocessor to be

resilient, and protect the integrity of protection processing and performance.

Independence provided the following benefits:

- Systems become simple to design, install, and commission with the assurance of independent actions;
- A failure of any component or unwanted transient (earth on battery incident, for example) in one system (Main 1, for example) does not impact the performance of the other system (Main 2);
- There are more reliable indications of fault type for electromechanical technology;
- Periodic testing and troubleshooting of each scheme can occur individually while the feeder is in service without compromising the protection of the feeder;
- All actions are traceable to particular equipment. For the previous example, the diodes joining the two battery banks allowed a bus trip signal to travel from Main 1 to Main 2 circuit and confuse the CB fail function and the investigation;
- Contact race problems of old technology equipment are significantly reduced.

Does the future hold true independence for protection schemes?

In the past, transmission utilities required two diverse, redundant, and independent protection systems where as little as possible was common between the two schemes. Communications engineers, particularly those involved in applying IEC 61850, are today challenging this question of independence. To enable interoperability between different manufacturers' protective devices, information technology engineers devised a communications protocol that was self descriptive, meaning that each piece of data that was communicated between two or more devices carried not only the required data but attached to these data a full description of the data (from the origin of the information, when it was generated, the quality of the data, etc.). IT engineers have proposed that this protocol be used for teleprotection schemes. They have reasonable expectations that this protocol will:

- Be more complex than binary signaling;
- Have public and private areas for special manufacturer application(s);
- Eventually have a number of upgrades.

The question we must ask about this approach is, "If both independent protective devices used this as the communications media for a teleprotection scheme, are the two schemes truly independent and dependable?" If we assume that there is a software issue with regards to the teleprotection communications protocol or its implementation, there could be an unwanted outcome because both independent schemes use this common teleprotection protocol. This concern is based upon the following:

- Divergent paths of communications technology, and a protection protocol that is an 'accommodated user'. The main concern is how rerouting of signals will affect this protocol and relay processing for security, speed, and dependability;

- Different interpretations of the IEC 61850 Standard's specification that have caused initial failed interoperability of GOOSE messaging among vendors;
- Past failures in the infant stage of any product cycle and probability of upgrades. This will require more complex software engineering;
- The variability in quality of implementation by manufacturers. One example with a current differential datagram: a manufacturer changed the datagram's protocol in a very minor firmware revision. Two differential relays were installed with different minor firmware versions, and this resulted in increased spill current under load. A through fault caused high spill current and tripped the feeder;
- A standardized protocol that makes it simpler for terrorists to 'hack the system' and cause protection misoperations.

Supporting evidence shows utilities being reluctant to use the GOOSE message solely for direct tripping of CBs and that there has been initial false tripping of early current differential schemes as a result of lost data telegrams or loopback in the communications network (see Appendix 8: Current Differential Protection).

It is the opinion of the authors that, if redundant protection schemes are to be truly independent, they (and their communications media) must be designed to have as little in common as possible to minimize common modes of failure. Remember the adage: "The proof of the 'Swiss cheese' is in the eating."

## XV. APPENDIX 8: CURRENT DIFFERENTIAL PROTECTION

A simple description of current differential protection (87L) is that relays at each end of a feeder measure current at time-stamped intervals ( $S_K, S_{K-1}, S_{K-2} \dots$ ) and send these data securely in a telegram (data packet) to the other relay(s). Each relay time correlates data samples, determines independently if an internal fault exists, and trips (see Fig. 41).

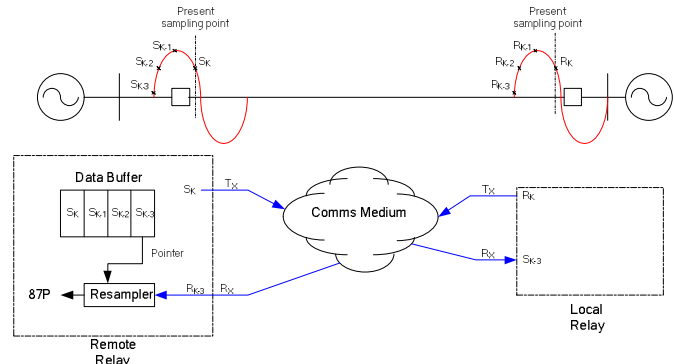


Fig. 41. Simplistic sketch of a current differential protection scheme

A very important question is whether 87L protection is biased to dependability or security? The answer depends upon the overall design as follows:

- In basic form, all differential protection systems can be prone to synchronization or data integrity problems.

It is therefore good practice to provide a supervision or check function on trip output;

- Numerical 87L relays provide many features to supervise the 87 (trip) output. Some examples of supervision include distance element, symmetrical component element(s), overcurrent, and minimum number of sequential trip decisions. The relay's functionality enables protection engineers to optimize dependability and security;
- The integrity of a communications system is one important area for these reasons:
  - Generally, communications staff operate their system without isolation of 87L relays. Experience has shown that some relay manufacturers have poor integrity checks of telegrams and data or software bugs that produce an incorrect trip when the communications system is reestablished;
  - Efficient work practices require the removal and return of one relay from the 87L scheme without isolating the remaining relays. The previous comment about relay manufacturers applies.

The main advantages of current differential overdistance schemes are as follows:

- Unit protection with reasonably constant tripping time over the feeder;
- Virtually no coordination requirements between ends and minimal setting requirements;
- No impact on security from load encroachment or power swings. The feeder, therefore, could have higher load transfer capability;
- No minimum length of feeder (distance relays are generally applied to feeders longer than several miles). However, long feeders may need a higher pickup setting because of appreciable charging current (unless compensated) and longer tripping time;
- Insensitive to arcing faults, current reversal, and mutual coupling effects;
- Interrelay signaling functionality enables secure, additional protection/control functions such as DTT, inhibit autoreclose. Generally, eight bits are available;
- Commissioning is performed on the scheme, and the local relay can display the remote relay's quantities.

The disadvantages of current differential to distance schemes are as follows:

- Greater bandwidth (56/64 kBoard) and a low bit error rate digital communications system are necessary, impacting accessibility and cost;
- Tripping is slower than Zone 1 distance and it is proportional to signal propagation delay time;
- Communications protocols are usually manufacturer/model/firmware specific, so the same relay must be installed at each end;
- The first generation differential relays required that the communications channel delay be symmetrical (i.e., the send and receive time must be the same), have simple backup protection, or have an additional

device. Second generation relays negate these disadvantages because of their use of a GPS time reference, their accommodation of route switching, and full distance protection;

- Phase differential elements have limited sensitivity for resistive faults. Therefore, sequence differential elements often complement these elements. However, this requires dedicated logic to detect CT saturation or line energization;
- CT performance must be considered in application. Most relays provide a bias characteristic to overcome CT saturation;
- No backup capability for uncleared, external zone faults unless specifically provided. Two events of thermally damaged 80 MVA transformers and a fallen 66 kV feeder resulting from failed LV protection or an open-circuited substation battery during a trip execution testify to this need. Backup protection is time graded over the slowest CB fail protection or under plant thermal rating.

Numerical current differential relays can provide the following:

- For two-ended feeders, these relays offer hot standby operation where two communications systems are used and synchronization is maintained for both. Therefore, if one system fails, the standby is instantly operational;
- For three-ended feeders with duplex communication systems, the scheme can operate with one system failed;
- Accurate time stamping with the use of GPS. This minimizes the synchronization process between relays and, therefore, increases scheme availability;
- The possibility of two-ended fault location;
- Backup protection functions such as full distance, directional overcurrent, and earth fault, etc.
- Customized logic that enables the strategic use of the following protection functions according to the mode of communications system loss or failure – routine maintenance, loss under load condition, loss or failure during a detected fault. Additional timers are available for use with Zone 2 distance element pickup to enable strategic use for coordinated tripping.

## XVI. APPENDIX 9: PRESENT ENVIRONMENT AND DIGITAL COMMUNICATIONS

This appendix looks at the environment in which DCB schemes operate in the 21<sup>st</sup> century. Should either the permissive transfer tripping scheme or current differential protection (with a suitable backup strategy) supersede DCB schemes as a first choice protection?

### *A. Network Growth and the Electricity Market*

Protection engineers provide a very valuable service to society for the reliable supply of electricity, and as society's expectations change and as technology enables, engineers should review and improve this service.

Electricity is now fundamental to standard of living, and society demands 24-hour, seven-day-a-week availability. In addition, the quality of electricity is being scrutinized and specified (e.g., power quality standards are being prescribed). From these drivers and as a result of governments selling off electricity assets, the electricity market and regulators have evolved. In Australia, the ‘wires’ (distribution and transmission) are seen as monopolies, and the Australian Energy Regulator (AER) has taken a proactive approach to driving electricity charges down through rewarding efficiency and setting revenue rates, capital, and operational expenditure by a budget/performance review process every five years. Additionally, the Regulator each year:

- Can inflict a \$5M penalty or award as much as a \$5M bonus for network service performance based upon the number of outages in two classes: events greater than 0.2 ‘system minutes’ or greater than 1.0 ‘system minutes’ [9];
- Will publish the operational performance of wires organizations.

Obviously, protection plays a major part in network service performance. These initiatives actually promote the role of protection because of its reliability function. Relays can enable faster restoration by providing timely event and disturbance records over remote communications media to network operators.

In parallel, the electricity network has grown quickly, and there have been increased interconnections to remote network(s) in other states or provinces.

This growth causes the following:

- Dissection of long feeders into shorter lengths to suit new load centers and to improve security of supply/network stability.
- The size and number of transformers in substations increase and their impedance (specifically X/R ratio) increase. The consequences are increased fault levels and more arduous plant requirements (especially for CBs and CTs).
- The size and number of generators in the electricity network increase. The consequences are increased fault levels and more arduous requirements in substations or switchyards;
- Eventually, there are additional parallel feeders, series capacitor installations, or higher transmission voltages to supply more power, sometimes over congested feeder easements;
- Load encroachment and power swing problems for distance protection, which can reduce load transfer capability for the feeder;
- The interconnection to remote network(s) in another state or province can cause more operational problems and possible society/ political repercussions. The most spectacular are major blackouts of varying magnitudes. One event was initiated by a protection misoperation in one state of the interconnected grid of eastern Australia. Underfrequency load shedding occurred in all five states to maintain network

stability. The news media and politicians were bewildered but incensed at these “unrelated blackouts”.

Additionally, the wires’ communications networks have grown to suit network expansion and are being modernized as a result of the fast pace of digital technology. Two key drivers are OPGW and OPPC, which offer huge opportunities and high performance for each feeder and commercial traffic. The results can be very reliable protection signaling and possibly redundant, independent paths for signaling.

Now from within the framework of this challenging electricity market environment and network growth, let us examine the DCB protection scheme.

### *B. DCB scheme and teleprotection*

This scheme’s principal advantage was that the teleprotection signal was sent over the unfaulted feeder. This was important in the 20<sup>th</sup> century, during which analog PLC communication was widely used and was “subject to strong transient noise at the onset of the line fault until the arc has established, followed by an immediate increase in signal attenuation due to the short circuit of the faulty phases(s). During the interruption of the fault current, noise is produced again by the operation of CB.” [13] DCB schemes overcame this problem and were biased to dependable protection operation rather than to security. To improve security, DCB usually employed duplicate blocking signals and enabling by the communications systems’ channel OK (Guard function).

Additionally, it is common practice to apply the same protection schemes for parallel feeders to power stations, load centers, etc. A similar approach may be applied to a substation or switchyard that then expands to become a major node in the network as a result of load growth. For example, one substation that initially had four generators now has 11 generators plus nine feeders with DCB protection. The important point is that the DCB scheme on the faulted feeder must trip quickly AND all DCB schemes on feeders supplying fault current, must block tripping (i.e., be secure). We can describe this as double jeopardy, where one event can cause more than one result and lead ultimately to customer loss of supply or network instability. Clearing a fault preserves network stability, but tripping healthy feeder(s) can produce cascaded tripping of overloaded feeders, which results in network instability. One of the field cases approached this outcome.

Communications systems play a critical role in teleprotection for speed, reliability, design, and installation cost aspects. We can argue that the biggest impact upon transmission protection has been digital communications systems and the opportunities that these provide numerical current differential protection and, from this, inter-relay signaling for distance and directional relaying. Interrelay signaling enables wide-area control schemes and increases the quality of protection (no discrete protection signaling units (PSU) are necessary). Modern communication systems offer the following benefits:

- High security and fidelity, fast signaling, increased number of signals, status information of any communications system (no hidden failures), these are uncovered prior to the use of protection);
- Failover capability of communications system to redundant path(s);
- Multifunction use of communications system (SCADA, protection, internal telephone, etc.) and resulting low incremental cost for protection signals. Analog PLCs could provide about four high-speed signals, whereas fiber is relatively unlimited in quality and in number of signals and paths. In any case, signal redirection must be compatible with protection requirements and relays;
- Remote interrogation of relays, dedicated direct fiber for possible lease to media, data, communications companies (commercial traffic) who usually require redundant systems. This could be beneficial to increased dependability of teleprotection ( see Section V. Importance of Testing).

A DCB schemes bias to tripping has unfavorable consequences to society's requirements and to the Regulator's "reward" systems. These consequences that are clearly visible and can be appreciated by senior management. Thus, there are now financial and reputational considerations (the Regulator's website, ITOMS™, for example) to protection. We can overcome the principle advantage of DCB through careful design that uses digital communications systems and the capability of numerical relays to operate backup protection and/or hot standby communications ports. It is obvious that a permissive distance scheme (with digital communication) and current differential protection does not present the issue of double jeopardy that we discussed previously.

### C. OPGW

It is worthwhile discussing the reliability of OPGW, because this is the preferred communications medium for Australian transmission utilities. Optical fiber composite ground wire provides the shielding of HV conductors from lightning strikes together with the benefits of a digital communication. OPGW contains multiple optical fibers (OP) in a metallic tube that is surrounded by layer(s) of galvanized steel wire (GW) or aluminum coated steel wire (ACSR). Stainless steel tube is more reliable than aluminum tube, as the photographs illustrate. OPPC (Optical Phase Conductors) are similar, but these are outside the scope of the present paper.



Fig. 42. OPGW construction

Obviously, OPGW is installed above the feeder and shares the same route. Generally, two GW are installed for feeders operating above 100 kV to give the required lightning shielding performance. The installed cost for OPGW (48 fibers) is about \$US 7000 per km per ground wire on new feeders.

### D. OPGW Reliability

Duplicated protection schemes require two independent communications systems. One system can use OPGW, and the remaining system could use any one of the following:

- A different fiber within the same OPGW. This is not recommended because of the possibility of common mode failure. Examples of such failures include the following:
  - Fig. 1 shows a fiber splicing box that filled with water because of porous seam welds. The water eroded the fibers' aluminum tube, which then compressed the fibers and grossly attenuated the signals. The design should have a seamless 'top hat' with a skirt below the bottom gland plate;
  - A current differential relay alarmed for a communications failure before the communications equipment issued any such alarm. The fiber in OPGW was suffering creep as a result of a design fault (swaying, expansion/contraction of OPGW caused movement and, therefore stretching, in fiber);
  - Incorrect installation of OPGW, especially the tensioning process and quality of splicing fibers.
- An alternative route via a third feeder or a composite route through multiple feeders;
- Use of two OPGW on the same route;
- Other communications media such as microwave, radio, lease lines, etc.

The test for true independence is whether a single failure event can prevent tripping during a fault or a reclose event. Credible events include the following:

- Lightning striking the OPGW and burning through the wire, tube, and fiber(s). The historical evidence shows that lightning may burn through a wire strand but that

the tube and fibers are not affected. Because of OPGW swinging in the wind, the two ends of the broken strand unwind and eventually cause an earth fault with a feeder conductor. The GW remains mechanically sound. Because Queensland has a high lightning ground flash density and 13,000 circuit km of overhead conductor, an average of 10 OPGW and GW fault events occur each year;

- Ground wire breakage can result from joint compression failure, over tensioning, and tower attachment failure. Quality design and installation practices can minimize the first two failures. Tower attachment failure usually results from the mechanical attachment carrying induced current, lightning current, or fault current. It is possible to overcome this simply by terminating the GW with an insulator and providing a suitable electrical connection;
  - OPGW fails because of fault level creep near the substation. The fault current exceeds the rating for the GW, which heats up and sags into the feeder. This cause should be managed effectively because of its related impact upon the substation;
  - Airplane or helicopter crashing into feeder and severing the OPGW. A small airplane scenario is feasible in such areas where there is crop dusting. The small helicopter scenario is feasible because utilities employ aerial cleaning or maintenance. For these scenarios, the greatest probability is that the feeder and OPGW will remain intact and that protection will operate correctly.
  - There were reported events of larger aircraft such as military planes and helicopters colliding with lines/towers which were cut or fell to the ground (see Fig. 44). A quick calculation shows that it is questionable that conventional PTT teleprotection could respond quickly enough before being cut. Obviously, a long feeder has a higher probability of such an occurrence;
  - The Tokyo blackout of 14 August 2006 resulted from a crane on a boat hitting 275 kV feeders. Obviously, mobile cranes (either on land or water) can cause feeder faults but, by its position, the OPGW will survive and operate correctly;
  - Tower(s) collapses as a result of abnormal wind or ice loading, tower footing failure, age, motor vehicle accident, act of terrorism. Experience gained from six tower collapse events has shown that OPGW can remain intact and that the fibers can remain operational (stretched but with increased attenuation)—see Fig. 45. A key design factor is whether the tower—GW attachment will allow the wire to pull through and relieve the load. A key operational factor is that the protection must only operate for initial collapse and any autoreclose operation (if not inhibited by protection and communications alarming).
- Experience from a single tower footing failure showed

that the suspension tower stood on three legs and would have continued, provided no further abnormal condition occurs.

- A surprising statistic is that a tower collapse could occur, on average, every five years in a large utility. This depends upon the utility's total number of towers (as many as 50,000, for example), age distribution (to 50 years old, for example), maintenance regime, the voltage level, and environment (high winds, salty/tidal areas). Therefore, it is a probable event;
- OPGW fails as a result of extreme intensity bush fires, as Australia recently experienced in 2007 and 2009 (see Fig. 46). Reports indicate that the fibers were not damaged and that they continued to operate correctly;

Single-mode fiber (class G.652 ITU) presently has a maximum length of 120 km before amplifiers are necessary to boost the signal. The amplifier reliability is manufacturer specific, but our experience has been very good.

Therefore, OPGW cannot give absolute reliability, especially for a long feeder, but it is immune to noise induced from a fault and requires a catastrophic event for it to fail during a feeder fault.

### E. Digital MUX

Australia uses SDH and PDH (E1) communications systems, while the USA and Canada use Sonet and PDH (T1) communications systems. This section will look at an SDH and PDH (E1) system, such as that in Fig. 43.

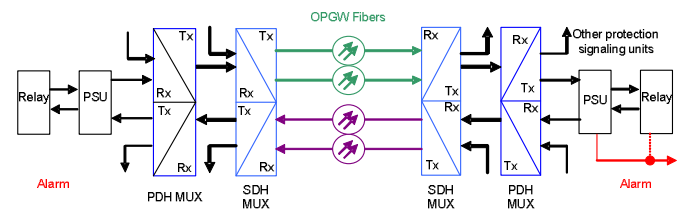


Fig. 43. A simplified sketch of a SDH and PDH system and teleprotection signals

The very high reliability of the communications system is achieved through the following:

- Use four fibers between SDH MUXs, instead of only using two fibers, to achieve dependability for commercial traffic. The SDH MUX transmits on the fiber pair, and the receiving SDH MUX transparently selects the better quality signal for processing. This is called hot standby or 1+1 redundancy (commercial communications companies use up to 1+5 redundancy);
- All the MUXs are IEDs and have self-diagnostic, alarming and performance-reporting capabilities. Reported unavailability is about two seconds per year for each MUX (hardware quality dependent). The hardware failure rate is similar to numerical protection relays (approximately five units per year for about 1000 PDH MUXs and 150 SDH MUXs);
- Independent transmit and receive ports;

- The independent operation of each half of the system such that one half may fail (green fibers) and the other half (purple fibers) can be set to remain in operation or shut down. The relay receiving the signal will receive the failure alarm and not the sending relay. This alarm could be used to initiate a strategic backup action;
- Redirecting the signal around the SDH ring if the shorter route fails. Achieving this requires careful design and setting;
- Fibers and routes into and within the substation that are designed, terminated, installed, and maintained under quality assurance practices that minimize common mode failures.

#### F. Summary

- A literature search found no quantitative statistics, but a review of utility MUX reports, hardware failure reports, and communications system reports from tower collapse events revealed that the digital communications system had a much higher reliability than analog PLCs. Therefore, the dependability of a digital teleprotection scheme will be superior to analog PLCs where the features of digital communications systems and numerical relays are exploited. This is largely because OPGW is a high reliability carrier, immune from fault disturbances unless the tower collapses or large aircraft hit it directly. This reliability decreases slightly as the route length increases because of the higher probability of these accidents and the increased number of fiber joints or amplifiers;
- Digital communications systems have greater reliability, especially when designed for commercial traffic, and they can switch to alternate fiber/routes to further increase reliability;
- Numerical relays can offer additional protection functions that can either operate in parallel to or switch within 20 ms from main protection in accordance with customized logic. In addition, their additional timers enable the implementation of multiple time-grading strategies for backup protection;
- IEDs provide comprehensive self-diagnostic functions and alarming that increase reliability;
- Electricity network growth can provide additional routes for teleprotection signals; their reliability must be determined in conjunction with communications engineers.

The previous discussion indicates that, when digital technology is based upon the purchase of quality equipment that is expertly designed, installed, and maintained, it has the capability to supersede DCB as a first choice teleprotection scheme.



Fig. 44. A failed FO splicing box showing that the rusted stand has broken from the base



Fig. 45. Tower and feeder damage from impact of large helicopter (photo source unknown).



Fig. 46. One of seven collapsed towers resulting from a storm cell—OPGW was stretched but still operational



Fig. 47. Collapsed tower as a result of Cyclone Larry (category 5 wind speed)—GW was broken at one location



Fig. 48. Collapsed tower resulting from a major bush fire—GW was intact. (No fibers in GW)

## XVII. BIBLIOGRAPHY

- [1] Clause S5.1a.8, Chapter 5, Australian Electricity Rules (Ver. 30); <http://www.aemc.gov.au/Electricity/National-Electricity-Rules/Current-Rules.html>
- [2] GEC Protective Relay Application Guide, Chapter 12.
- [3] SEL 421:Reference manual, Fig 1.68, page R.1.112, date code 20090715.
- [4] E.O. Schweitzer and J. Roberts, *Distance Relay Element Design* : P.M. Anderson, *Power System Protection*. New York: IEEE Press/McGraw-Hill, 1999.
- [5] Lewis Blackburn & Thomas J. Domin, *Protective Relaying Principles and Applications* ISBN 1-57444-716-5 J. CRC Press, 2007
- [6] G. Benmouyal and J. Roberts, "Superimposed Quantities: Their True Nature and Application in Relays" in *1999 26th Annual Western Protective Relay Conference Proceedings*.
- [7] IEEE Std C37.111-1999 IEEE Standard Common Format for Transient Data Exchange (COMTRADE) for Power Systems
- [8] <http://www.aer.gov.au/content/index.phtml/itemId/717931>
- [9] I. Stevens, "Testing Philosophy - the numerical relay perspective", *Australian Protection Symposium 2008*
- [10] "NERC System Protection Initiative" Spring 2009, PAC
- [11] S. Read, "Fiber optic materials, strategies and structures for new era substations" CIGRE SEAPAC 07.
- [12] "Protection using Telecommunications" Ch 4, CIGRE, JWG 34/35.11, 2001

## XVIII. BIOGRAPHIES

**Ian Stevens** holds the position of Principal Consultant (Protection and Metering) in Powerlink Queensland (an Australian transmission corporation). Ian has experience in design, evaluation, testing, procuring and performing investigations in protection and metering fields. He was a member of drafting committee for Chapter 7 (Revenue metering) of (Australian) National Electricity Code and a past member of Australian Standards committee ET/5 for environmental testing. Prior to joining Powerlink Queensland in 1980, Ian worked in Australian and New Zealand distribution authorities.

During 2000, Ian was heavily involved in the development of a new substation secondary system which utilized the functions of protective IEDs. During 2005, Ian is participating in investigation teams to implement power quality metering and introduce and design substations based upon IEC 61850.

Ian has received two innovation awards from Powerlink Queensland.

**Bogdan Kasztenny** is a principal systems engineer in the R&D department of Schweitzer Engineering Laboratories, Inc. He has 20 years of experience in protection and control, including his ten-year academic career at Wroclaw University of Technology, Poland, Southern Illinois University, and Texas A&M University. He also has ten-years of industrial experience with General Electric where he developed, promoted, and supported many protection and control products. Bogdan is an IEEE Fellow, Senior Fulbright Fellow, Canadian member of CIGRE Study Committee B5, and an Adjunct Professor at the University of Western Ontario. He authored about 200 technical papers and holds 16 patents. He is active in the Power System Relaying Committee of the IEEE and is a registered professional engineer in the province of Ontario.

**Normann Fischer** received a Higher Diploma in Technology, with honors, from Witwatersrand Technikon, Johannesburg in 1988, a BSc in Electrical Engineering, 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 Eskom's Protection Design Department for three years. He then joined IST Energy as a senior design engineer in 1996. In 1999, he joined Schweitzer Engineering Laboratories, Inc. as a power engineer in the Research and Development Division. Normann was a registered professional engineer in South Africa and a member of the South Africa Institute of Electrical Engineers. He is currently a member of IEEE and ASEE.