Back to Table of Contents

HIGH-SPEED DISTRIBUTION PROTECTION MADE EASY: COMMUNICATIONS-ASSISTED PROTECTION SCHEMES FOR DISTRIBUTION APPLICATIONS

Roy Moxley and Ken Fodero
Schweitzer Engineering Laboratories, Inc.
Pullman, WA USA

ABSTRACT

High-Speed Distribution Protection Made Easy: Communications-Assisted Protection Schemes for Distribution Applications

Communications assisted protective schemes in transmission applications have been in service for decades. Recommendations for scheme application are well established, depending on the type of channel. Communications typically used for transmission line applications include power-line carrier, microwave, and optical fiber.

With more emphasis being placed on distribution system reliability there is a need to establish protection methods for the varying communications being used on these systems. By their nature, distribution lines are different from transmission lines. They are generally shorter, they have more tapped loads, and load currents are frequently on the same order of magnitude as fault currents. Communications systems are also different from those used on transmission lines, with associated differences in errors, outages, and signal-transmission reliability.

This paper examines different communication paths for protection signals, such as spread-spectrum radio, fiber-optic cable, phone lines, and copper pilot wire. Data transmission statistics with performance measures are given for each type of communication. Based on the communication characteristics and its performance during faults, different protection schemes are studied with total clearing times given for each scheme. The consequences of communications failure on each type of scheme are examined, including the possibility of misoperation, as well as backup clearing times.

INTRODUCTION

High-speed tripping has always been a prime qualitative measure for transmission relaying systems. The need to maintain power transfer capability and reduce fault damage to transmission lines and equipment mandated and justified large investment in high-speed relaying and communications equipment. Protection schemes were created to mitigate communications limitations and preserve high-speed operation under as many conditions as possible [1].

In transmission systems, different protection methods are used with different communications systems. On/Off power-line carrier communications (PLC) is commonly used with blocking schemes. Frequency-shift keying (FSK) of PLC or microwave is used with permissive schemes. The scheme is selected to complement the strengths or weaknesses of the communications. With on-off carrier it cannot be certain that the signal will be sent when triggered, but because of the wide bandwidth used it is very fast. This is natural for a blocking scheme, with the consequence of possible overreaching if the blocking signal is not sent (and received), but avoiding a failure to trip under those circumstances. With FSK schemes there is a continuous signal sent, with a change from “guard” to “trip” when keyed. Because a guard signal is always received, there is confidence that a trip signal, when needed, will also be sent and received.

HIGH-SPEED REQUIREMENTS FOR DISTRIBUTION SYSTEMS

Just as high-speed tripping is important to the stable and secure operation of the bulk transmission system, it is important to the distribution system although for different reasons. Individual customers have operating systems that require reliable power. There are also voltage conditions that can be aggravated by delayed fault clearing. For example, in areas with a large amount of air conditioning load or induction generators, such as some older wind farms, the drop in voltage caused by a fault can initiate a voltage collapse [2].

Consider two power systems: one a 500 kV system transmitting 1000 MW to a large metropolitan area as part of an interconnected system (Figure 1), the other a 13.8 kV line transmitting one of two feeds to a large industrial park (as shown in Figure 2). The distribution circuit could be two radial feeds from different sources or part of a distribution network similar to that described in Reference [3].

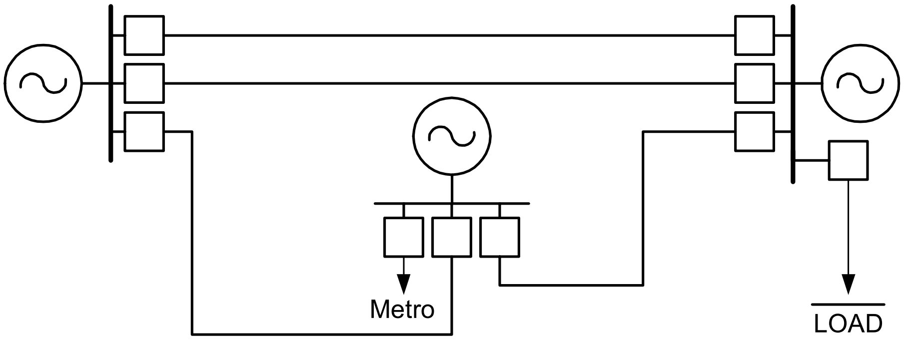

Figure 1 Interconnected Power System For Bulk Power Delivery

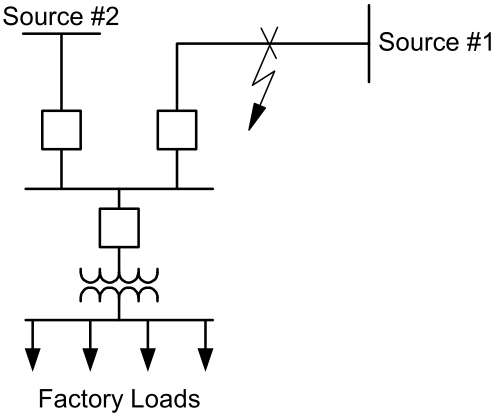

Figure 2 Factory Load With Two Independent Feeds

In the case of the bulk power system, a fault near a transmission bus on one of the power lines will compromise the ability to transmit power across the entire system. In order to maintain system stability, fault clearing must be completed in a short time, typically from 12 to 20 cycles.

In the case of the distribution feeder to the industrial load, system frequency stability is not a consideration, however other factors may necessitate high-speed tripping. The most important factor may be keeping motors in the factory on line. According to a survey published in the IEEE Gold Book [4], 25 percent of industrial plants must completely restart production if service is interrupted for more than ten cycles. The survey goes on to say that the average restart time is 17 hours, indicating a severe economic disruption for a very brief outage. While it is well understood that motor torque goes down with the square of the voltage [5], the problem is with the motor contactor, not the motor. When the contactor drops out the motor will stop. Many processes require clearing the driven device, such as the grinder, conveyer or extruder, once the motor stops because it does not have sufficient torque to start under full load. The Information Technology Industry Council has established a curve, the CBEMA curve, that indicates a generally acceptable voltage range for power delivery.

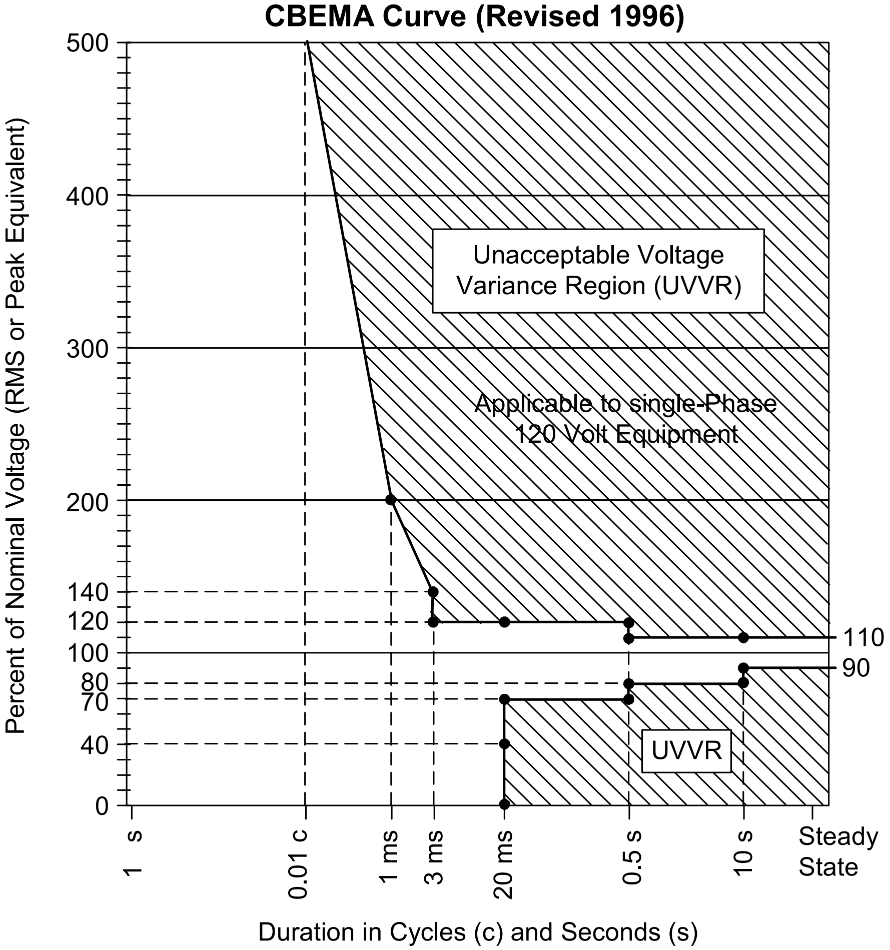

Figure 3 Voltage Acceptability Curve [6]

This curve is more restrictive than a requirement for motor contactors, but it has the advantage of showing the degree to which a voltage reduction can also cause problems on a customer's system. While multiple feeds, or a distribution network will improve overall service reliability, it can increase the number of voltage sags or interruptions by increasing the circuit exposure.

Fault location on the line makes a difference in what the resultant voltage is at the customer load. Fault resistance and the load's ability to maintain voltage at its own terminals is also a factor. The

CBEMA curve shows though, that very high-speed tripping (for a distribution system) is necessary to reduce the time spent in the UVVR region to between 20 ms and 0.5 seconds.

The problem of operating speed requirement is compounded by the speed of the distribution breaker as compared to the transmission breaker. While typical transmission breakers will interrupt fault current in two or at most three cycles, distribution breakers will usually have an interrupt time of five cycles. This leaves a total of five cycles for the relaying system on the incoming distribution feeder to operate for a fault to make sure the voltage recovers quickly enough to prevent contactors from dropping out.

It is possible for a instantaneous or time-overcurrent unit to operate in less than five cycles (80 ms) as shown in Figure 4, although such speed requires using the 0.5 time dial setting.

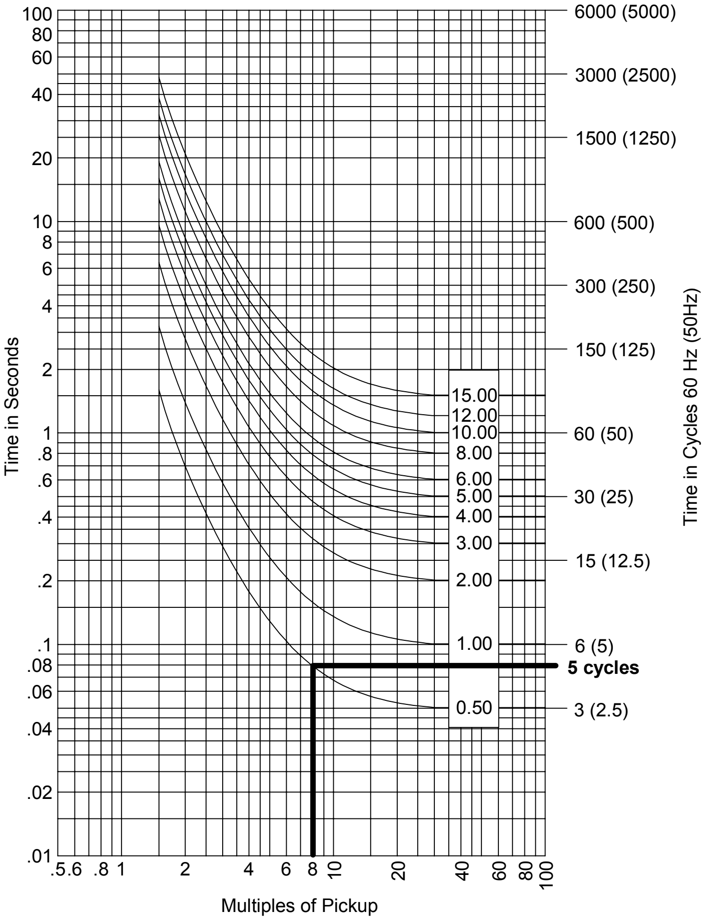

Figure 4 Inverse Time Curve

The problem that comes up is one of coordination. Even though these overcurrent units can operate with the speed required, under practical conditions of coordinating with downstream devices, the speed is much reduced. Figure 5 shows operating times of 34.5 kV overcurrent-based fault clearing at a large utility [7]. These are all the faults on the entire 34.5 kV network during an 18-month period.

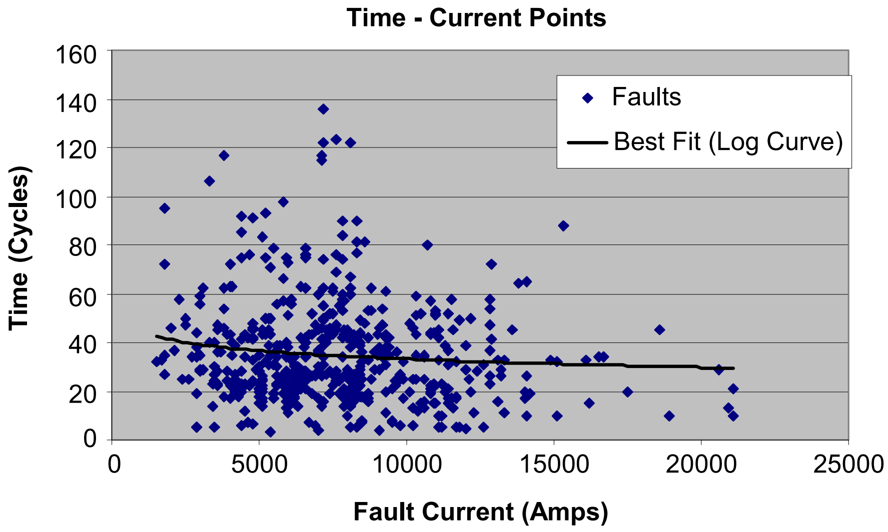

Figure 5 Typical Feeder Trip Time vs. Current

As can be seen, the average clearing time for a 10 kA fault is in excess of 30 cycles. In fact, only 32 out of 535 faults on lines with overcurrent relaying were cleared in 10 cycles or less.

Clearly then, overcurrent relaying is generally not able to operate fast enough to prevent major costs from being incurred at industrial loads on a distribution system. To get the necessary speed, some form of communications assisted tripping scheme is necessary. The question then is, what communications are available in a distribution system and what protection scheme works best with which communications system?

COMMUNICATIONS NEEDED

There are a number of new and traditional communications systems available today. Each has strengths and weaknesses that make them more or less suitable for different types of protection schemes.

A rigorous comparison of schemes using fault tree analysis [8] can be done for any given situation, but for distribution systems may be too time consuming. It may be reasonable to establish a standard, based on local conditions and needs, and use analysis to establish that standard. Choices for distribution system communications to improve operating times can include one or all of the following:

Direct Pilot Wire
Leased Phone Line—direct
Leased Digital Phone Line—CSU / DSU
Direct Fiber-Optic Cable
Multiplexed Fiber-Optic Cable
Licensed Radio
Spread-Spectrum Radio

Communication considerations include channel bandwidth and speed of signal transmission. These may limit the capability of a particular protection. For example a 9600 bps audio modem would not be suitable for a current differential protection scheme requiring 64,000 bps transmission capability.

Table 1 Typical Communications Device Delays

Device	Max Baud Rate	Time
Multiplexer	19200	2–4 ms
Audio Modem	9600	12 ms typical
Spread-Spectrum Radio	38400	4 ms
Fiber Modem	38400	< 1 ms
Leased digital Phone Line (CSU/DSU)	64000	5–20 ms

We will not examine microwave or power-line carrier for distribution protection in this paper. While there may be specialized applications where they could be used, they are generally unsuitable for distribution systems based on cost or physical considerations.

DIRECT PILOT WIRE, LEASED DIRECT PHONE LINE

As far as protection is concerned there is no difference between a directly connected pilot wire and one leased from a phone company. The availability of leased, copper phone lines is becoming difficult and preventing phone company switching of lines has always been an issue. The protection applied when using a directly connected pilot wire is virtually always differential. In the same utility study for overcurrent protection referred to earlier, pilot wire protection on distribution circuits provided clearing times of less than 10 cycles in 43 out of 57 faults. In those cases where the clearing time was greater than 10 cycles it was usually the result of coordinating delays on tapped lines.

While speed of pilot wire differential relays is sufficient, security considerations are a major issue. During a period where there were 57 correct trips there were 6 false trips and 4 failures to trip, all caused by pilot wire problems. This amounts to a 17.5 percent failure rate of the protective scheme caused by pilot wires being shorted, open, or reversed. This high failure rate clearly indicates that pilot wire monitoring should be considered an essential part of any pilot wire protection system.

While the cost to connect to a direct pilot wire is low, the cost to protect personnel and equipment from damaging surges is moderately high in terms of equipment and care in wiring. Neutralizing reactors are needed to prevent common mode voltages from appearing on the pilot wires. Typically these voltages are a result of ground potential rise, which can be thousands of volts. Induced voltages, typically a result of running pilot wires below phase wires, must also be prevented from operating relays. Mutual drainage reactors are needed to eliminate these induced differential voltages.

DIRECT CONNECTED FIBER

Point-to-point fiber optic has terrific operational advantages where it is available. Unfortunately for most distribution circuits, the cost of a dedicated fiber is prohibitive. As a rule of thumb, a fiber cable costs about one dollar per foot, depending on the number of fibers. A ten-mile line then would cost over $50,000 plus installation costs. Because of data transmission capability, where point-to-point fiber optic is cost justified it is usually used for current differential relaying. With no induced noise, ground potential rise, or other sources of interference, it is ideal for this purpose. For the most part though, the great data carrying capability of fiber makes it most suitable for multiplexed signals.

MULTIPLEXED FIBER

While fiber-optic cable itself is immune from noise sources, the terminal and multiplexing equipment can produce noise or momentary loss of signal. As noted in Reference [9] "Excessive bit error rates were immediately prevalent in the relay system as a result of the use of an unproven communications interface device intended to provide the optical/V.35 electrical signal conversion required between the differential relay and the SONET multiplexing equipment." Recorded bit errors exceeded 40,000 messages in a period of 118 days. The bit-error rates caused the relay scheme to indicate failed communications, which disabled the line protection on a regular basis. A new relay system using a direct C37.94 interface to the multiplexer operated without any bit errors for the first seven months of operation on five out of six installed systems. The sixth system experienced a 200 ms loss of communications, however, because it was a dual-channel system, protection was not interrupted. In instances where the security problems of the continuous data transmission required for differential communications cannot be reasonably worked out, it may be better to change the protection system to one more tolerant of channel failure, as will be discussed in a later section.

RADIO SYSTEM

For all the bandwidth, noise immunity, and operational advantages of fiber-optic protection, there are disadvantages beyond technical performance. In the words of a utility communications engineer, "If they bury it, someone will dig into it, if they hang it in the air, someone will shoot it." Because all of the radio equipment except a small antenna can be installed in a protected enclosure, radio has practical advantages.

Communications Quality Reports (Com Log)

Because both licensed and unlicensed radio systems can be impacted by many interfering factors it is important to continuously monitor those communications. Both the frequency of communication failures and their duration can have a significant impact on the selection of the protection scheme. For example one check of a communication report from a relay connected to a radio system revealed the following information (Table 2).

Table 2 Typical Radio Communication Report

Dates	Total Failures *	Relay Disabled	Longest Failure	Unavailability
7/16 – 8/22/2001	18	1	0 00:00:17.472	0.000006

When the communication report is requested from the relay the details of each of the events can be retrieved. While the summary above is useful, it can be especially important to get the date and time of each failure. This can be used to diagnose problems and achieve a solution or determine if no action is necessary.

This example is from a radio system that was in service for about a month. Other than a 17.472 second outage on 8/4/01, this system has operated very reliably. Using the date and time of the communication failures it was determined that the 17 second communication failure was not coincident with any power system fault. This is an important part of establishing the suitability of communications for protection.

SPREAD-SPECTRUM RADIO

Spread-spectrum radios use multiple frequencies in the 900 MHz and 2.4 GHz license-free ISM band. These radios are secure because they use proprietary synchronization methods between the transmit and receive ends that allow only a point-to-point connection. The advantage of this system is that once it is installed, there are no additional recurring costs, such as license or leasing fees. The complication is that because these radios use unlicensed frequencies, there is no guarantee that another user will not be using one of those frequencies. A typical spread-spectrum system “hops” between 25 different frequencies within the band (Figure 6). The time spent at any particular frequency is so short that if there is interference at that frequency there will be only a short period of channel unavailability.

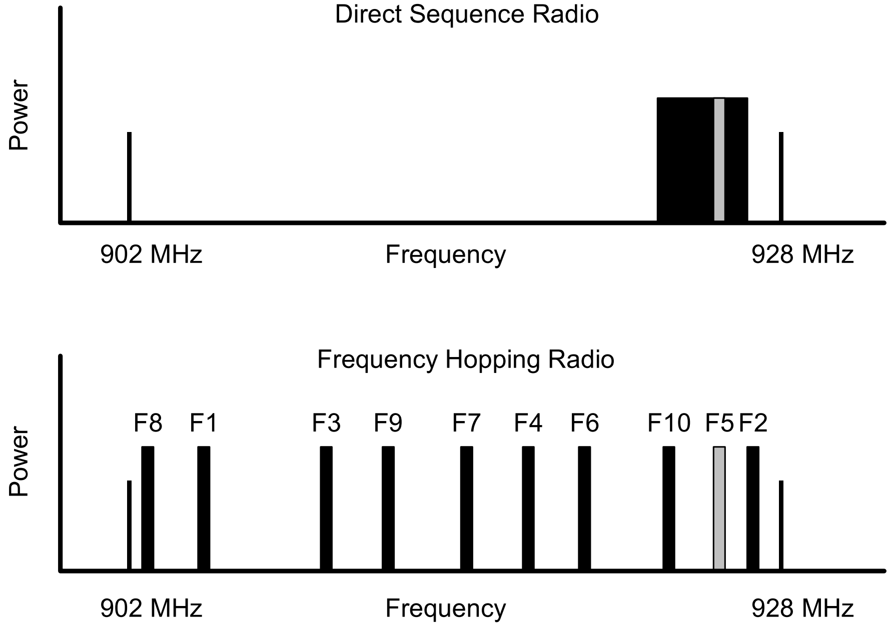

Figure 6 Interference to Direct Sequence and Spread-Spectrum Radios

There are two modulation types in use in the ISM band, frequency hopping and direct sequence. For direct relay-to-relay digital communications applications, frequency hopping is the most robust. Direct sequence is predominantly used for high-bandwidth applications, such as Ethernet.

Direct Sequence Communications may be blocked while an interfering signal is present. The symptoms range from reduced throughput to a complete loss of communications. Frequency Hopping Communications may be blocked only when a particular frequency collides with the interfering signal (F5 in Figure 6). The symptom is reduced throughput caused by short losses in communications. If particular frequencies are causing a problem, interference can be reduced by changing both the pattern of shifts between frequencies and the frequencies within a particular band that are being sent (Figure 7).

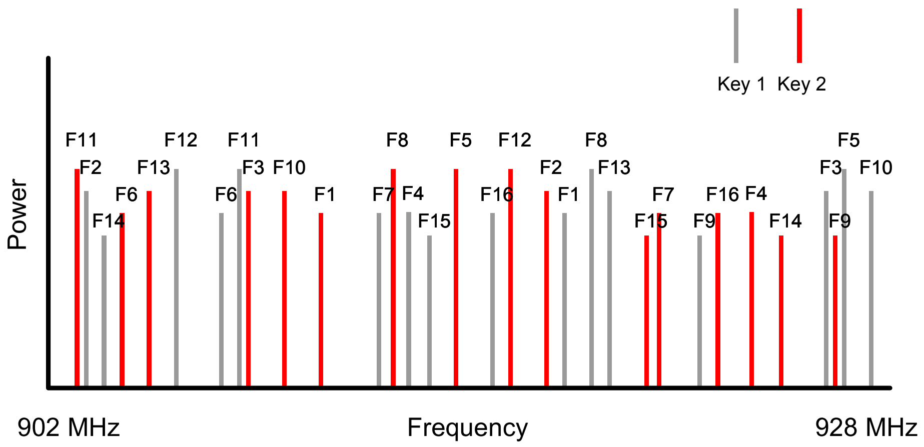

Figure 7 Avoid Interference By Changing Frequency Key

The probability of an interfering signal depends on the number of other users in the area. Because users do not require a license, the number of users will generally be proportional to the number of industries in a given area.

The change in availability over time is an interesting illustration of this congestion effect. The following three reports were received from a utility in a major metropolitan area on the Friday, Saturday, and Sunday before Thanksgiving. The communications logs show a significant improvement in availability as the weekend progresses (Table 3).

Table 3 Spread Spectrum Radio Unavailability

Dates	Total Failures *	Relay Disabled	Longest Failure	Unavailability
11/22/02 (Fri)	256	0	1.058 sec	.000320
11/23/02 (Sat)	256	0	1.054 sec	.000208
11/23/02 (Sun)	256	0	1.050 sec	.000094

* 256 failures is the maximum buffer length in the subject relay's report

Note that Saturday's total unavailability is 35 percent lower than Friday's and Sunday's unavailability is 71 percent below Friday's. Of course, we cannot rely on faults only occurring on weekends. This analysis can help pinpoint the root cause of communications failures, especially on a shared frequency. The other information from the report that can be very useful is the duration of the longest failure. While the unavailability of these spread-spectrum radios is much higher than for other illustrated radios, the longest failure is much shorter. The unavailability of the other radio is just 0.000006, a factor of 15 better than these spread-spectrum. Because the licensed radio is in a single narrow band however, just one problem with that frequency can lead to longer failures. In this case 17.472 seconds compared to just over 1 second for the spread-spectrum radio, even on Friday.

A smaller metropolitan area installed radios for protection communications on two lines of 15 and 23 miles in length. The communications report shown in Table 4 makes it clear that unavailability is not necessarily the only factor to be considered when looking at the suitability of the communications link. Here the unavailability is virtually the same as the large metropolitan area on a Friday, at 0.000035. What is different is that the longest failure is only 0.008 seconds in length. This delay is insignificant on a distribution system, as long as the protection system can accommodate many short communication outages. For example in this case a permissive scheme may be more suitable than a current differential scheme. The protection scheme must reliably continue to transmit "through" a communication outage.

Table 4 Small Community Spread Spectrum Radio Unavailability

Dates	Total Failures	Relay Disabled	Longest Failure	Unavailability
7/16/2003	256	0	0.008 sec	0.000035

The total hardware cost of a spread-spectrum system is typically less than the cost of conventional teleprotection systems. As demonstrated through various applications, these systems can be just as reliable as leased voice channels.

COMMUNICATIONS SYSTEM SUMMARY

The characteristics of the communications system impact its applicability to a particular protection scheme. Likewise, the protection scheme selected needs to take advantage of the strengths and accommodate the weaknesses of a particular communications system. As a comparison of general characteristics of the different communications systems that are reasonably available for distribution systems, we can make a table as follows:

Table 5 Qualitative Communication Comparison

	Direct Pilot Wire	Leased Digital Phone Line	Direct Fiber-Optic Cable	Multiplexed Fiber-Optic Cable	Licensed Radio	Spread-Spectrum Radio
Channel Unavailability (typical)	High	Low–Very Low (0.000007)	Very Low	Varies with interface	Low (.00001)	Med. (.00003)
Longest Failure (typical)	Very Long (days+)	Short, depending on service provider	Very Short	Short (0.2 s)	Medium (20 s)	Short (1 s)
Fault-Related Failure probability	High	Med / Low	Low	Very Low	Low	Low
Terminal Cost	Medium	Medium	Low	High	Medium / High	Medium
Path Cost	High	High	High	High / but Shared	Zero if License Held	Zero
Environmental Ruggedness	Medium / Poor	Medium / Maintained	Medium	Medium	High	High
Communication Speed (typical)	High (1–3 ms) plus interface time	Med (5–20 ms)	Very High (0.1 ms)	Med depending on # of nodes (2–4 ms)	Med (2–4 ms)	Med (4 ms)
Data Rate	Very low (4 kbps)	Medium (64 kbps)	Very High (4 gbps)	Med. (64 kbps +)	High (25 Mbps)	Med. (115.2 kbps)

Previous tabulations of this type [10] are useful but have not included relative cost, speed and other features. In distribution applications, cost considerations become very important. While an entire system can benefit from transmission protection improvements, the benefits from distribution improvements are much more local. Frequently it is the end user on the circuit that must pay for the improvement. Choosing the most cost effective solution, or offering options, can improve the energy supplier’s relationship with that end user.

PROTECTION SYSTEMS

Sometimes the protection requirements can determine the communications method and sometimes the communications availability will determine the protection system. Because cost is a very important part of most components of the distribution system, the choice and even the availability of communications for protection may depend on what is already available.

There are three basic communications schemes commonly used for transmission systems. They are:

Current Differential
Permissive Overreaching Transfer Trip (POTT)
Directional Comparison Blocking (DCB)

Of course there are numerous variations of these: phase comparison, permissive underreaching direct transfer trip, and unblocking schemes; but most of these are applicable because of the specific characteristics of power-line carrier or microwave communications which we are not considering. Let us examine the three main schemes for their applicability to specific communications paths.

CURRENT DIFFERENTIAL

There are two basic types of current differential. One simply sends all data to communicate all three phase currents from one end of the line to the other. The second combines the three phases into a single signal and communicates that for comparison with the other end. The main difference between the two is a factor of at least three times the data being transmitted (and hopefully, received). This factor ends up being more than three times the data because phases must be identified and then the message must be formatted for transmission with timing information. In a traditional (electromechanical) pilot wire differential scheme the comparison of the signals can be thought of as taking place on the wire itself, with either circulating current or opposing voltage indicating an operating or restraint condition.

Digital current differential has the advantage of being able to compare both the currents and the signal integrity in order to make the trip decision. In the case of the utility referenced earlier [7] many false trips on pilot wire relays can be traced to a combination of communications errors with external faults. This can be illustrated as shown in Figure 8.

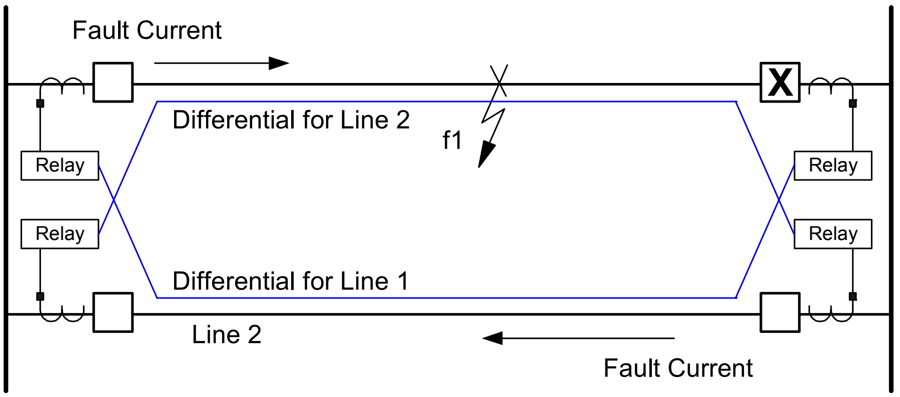

Figure 8 Power Lines and Communications

In this case the engineer is faced with a choice. The communications can be run either with the line being protected or with a parallel line. If a significant number of faults on the power line (f1) have the chance of disrupting communications, then problems will result. If a communications failure causes a failure to trip, then the path selection as shown in the figure would be a good choice, as a fault on line 1 with a communication failure will not cause line 2 to trip. One problem was that a shorted pilot wire, caused by the fault, caused the relays on line 2 to incorrectly trip for a fault on line 1. This circumstance can reduce or eliminate the benefit of a dual feed for a large industrial customer. There is no simple solution for this case if a short circuit in the communications can false trip, and an open circuit can cause a failure to trip, or even if the conditions are reversed and a short can cause a failure to trip and an open a false trip.

This real world example points out the importance of an assignable state for the protection if communications is lost. This capability can be used for both differential protection and other schemes.

For digital current differential protection, no current comparison should be made if the communications is not established as OK. This requires a “communications healthy” bit be a part of each message and protection-processing interval. The case described in Reference [9] shows the advantage of a system that does just this.

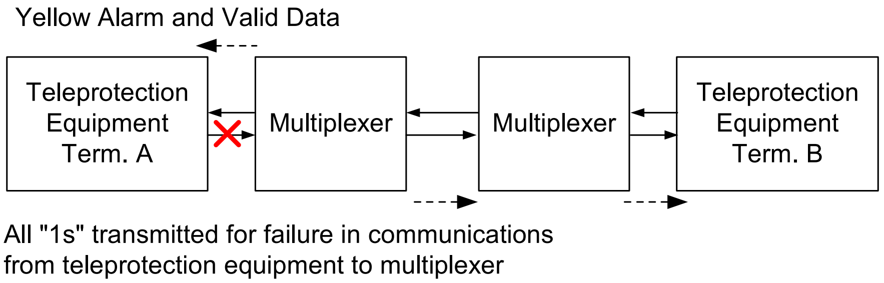

Figure 9 IEEE C37.94 Communication Standard

As described earlier, a compliant interface can drastically reduce bit errors even while establishing a system to handle those errors. The diagram in Figure 9 shows how an IEEE C37.94 compliant multiplexer and interface can identify that a loss of signal is indicated to both ends of the protected line. In this case, the protection equipment at terminal A recognizes that it is receiving healthy data, but that terminal B does not have healthy data. The protective equipment at terminal B likewise knows that it is not receiving healthy data. Terminal A can still operate at high speed for all faults, while terminal B can switch to backup mode. In the case of a double circuit feeder, such as Figure 2, there is now at least a chance to return to full voltage at high speed, even if one protection channel has failed.

PERMISSIVE OVERREACHING TRANSFER TRIP (POTT)

A permissive tripping scheme provides a means to limit the protective zone of a relay scheme (Figure 10).

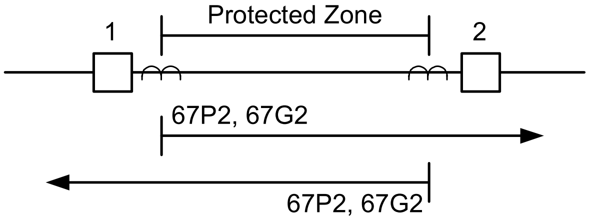

Figure 10 POTT Scheme Diagram

Just as a differential relay is biased toward tripping (unless action is taken as described above) if the communications channel is lost, a permissive tripping protection scheme is biased towards not operating if the communications is lost. The advantage of a POTT scheme is that directional elements can operate at very high speed. The protection system, as a whole, needs to address the possibility of a lost signal during a fault.

In transmission systems using power-line carrier, or other signal that has a high probability of lost channel during a fault, it is a common practice to include a short permissive window upon loss of channel. Immediately upon a loss of signal this provides a short time (typically 20 ms) that the relay can operate in a POTT mode even without a received signal. This can compromise security, but, depending on channel type, may be a very reasonable action.

In the case of distribution systems, the need for a permissive window on loss of channel can be eliminated if it is known that the vast majority of lost channel events will be very short compared to the overall desired tripping time. For example if the spread-spectrum radio system reported in Table 4 is in use it can be seen that the longest outage was measured at 8 ms. With a five-cycle (80 ms on a 60 Hz system) desired operating time for the relay scheme, the delay from a possible data loss still allows the overall operating time to be well within that desired. If, on the other hand, the communications scheme is more like that of the Table 3 report, with a possible loss of channel for one second, then a permissive trip window may be needed. Another factor affecting the need for a permissive window is the likelihood that a channel failure will occur at the same time as a line fault. While lightning can cause a very short noise burst, arc noise from a fault will generally not cause any loss of a radio signal between two ends of a line. Of course a raccoon climbing across an insulator will not interfere with a radio signal.

Another concern when using POTT schemes is that relays at both ends of the line must see the fault. This can reasonably be ensured on transmission networks, but on a distribution system there may be system connection possibilities that remove any infeed from one end of the line. This problem has been overcome by adding a second communications channel used with a blocking scheme [2]

DIRECTIONAL COMPARISON BLOCKING (DCB)

The inverse of a permissive scheme is a blocking scheme. Here a relay will trip unless a signal is received from the other end preventing operation (Figure 11).

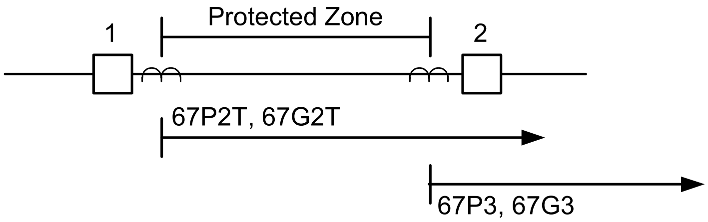

Figure 11 Directional Comparison Blocking (DCB) Scheme

A blocking element is biased towards tripping if the communications channel is lost. The cost to tripping time is that a small coordinating time delay must be added to the tripping element. This provides for the time necessary to send a signal from the other end of the line in case of an external fault.

If the communications signal is only sent when a fault is detected there is no way to ensure that a signal has not been received because of an internal fault or because of a channel failure. In transmission systems using power-line carrier, the problem is lessened by using a periodic checkback system and eliminated by using a frequency shift keying that sends a continuous signal and changes from trip to block during an external fault.

Table 6 Protection Scheme Comparison

	Permissive Overreaching Transfer Trip (POTT)	Directional Comparison Blocking (DCB)	Current Differential
Operating Speed	High (1.5–2 cycle)	Med–High (2–2.5 cycle)	Very High (1–1.5 cycle)
Loss of Signal (LOS) Consequence	Failure to Trip	False Trip	False Trip
LOS Mitigation	Add Trip Window	Continuous Channel Monitor	Continuous Channel Monitor
Typical Data Rate Required	9600–38400 bps	9600–38400 bps	56–115 kbps

SUMMARY

For applications requiring high-speed operation the selection of protection scheme and communications system are closely intertwined. It is critical that the protection engineer be aware of the probability and failure mode of the communications channel to ensure the proper operation of protection under the broadest conditions. Table 7 shows typical considerations when applying protection schemes with communications systems.

Table 7 Protection and Communications

	POTT	DCB	Current Differential
Licensed Radio	Proven Application	Proven Application	Complex Application, Check error rates and interface
Spread-Spectrum Radio	Proven Application	Proven Application	Not Recommended, Insufficient Bandwidth and Interface
Direct Fiber Optic	No technical problem, may be difficult to cost justify	No technical problem, may be difficult to cost justify	Proven Application, may be difficult to cost justify
Multiplexed Fiber Optic	Proven Application	Proven Application	Proven Application, Standard Interface and Monitored Communications Recommended
Pilot Wire	Not Normally Used	Not Normally Used	Physical Considerations, Ground Potential Rise, Monitoring, Path Routing
Leased digital phone—CSU / DSU	Proven Application	Suitable but not normally used	Under Investigation [10]

CONCLUSIONS

1. In order to ensure protection quality, communications should be monitored during normal and trip conditions and alarmed for prolonged failures.
2. The protection scheme must consider the speed and quality of the communications system.
3. Backup protection, even if contained in the primary relay, must be designed with consideration of the anticipated failure mode and rate of the communication system.
4. Protection logic values need to be assigned for the condition of channel failure to reduce possible false trips and failures to trip.

REFERENCES

[1] E. O. Schweitzer III, K. Behrendt, and T. Lee, “Digital Communications for Power System Protection: Security, Availability, and Speed,” presented at the 25th Annual Western Protective Relay Conference, Spokane, Washington, 1998.

[2] J.R. Roberts, T.L. Stulo, and A. Reyes, “Sympathetic Tripping Problem Analysis and Solutions,” presented at the 24th Annual Western Protective Relay Conference, Spokane, Washington, 1997.

[3] J. R. Fairman, K. Zimmerman, J. W. Gregory, and J. K. Niemira, “International Drive Distribution Automation and Protection,” presented at the 55th Annual Georgia Tech Protective Relaying Conference, Atlanta, Georgia, 2001.

[4] *IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*, (IEEE Gold Book) IEEE Standard 493-1990 (Revision of IEEE Std 493-1980), Sept. 1990.

[5] GE Industrial Power Systems Data Book. July 5, 1953, section .210 page 3.

[6] CBEMA Curve Application Note, Technical Committee #3 (TC-3) of the Information Technology Industry Council (ITI), 1996.

[7] R. Moxley, "Analyze Relay Fault Data to Improve Service Reliability," presented at the 30th Annual Western Protective Relay Conference, Spokane, Washington, 2003.

[8] G. W. Scheer, P.E. "Answering Substation Automation Questions Through Fault Tree Analysis," presented at the Fourth Annual Substation Automation Conference, Texas A&M University, College Station, Texas, 1998.

[9] D. Carroll, J. Dorfner, T. Lee, K. Fodero, and C. Huntley, "Resolving Digital Line Current Differential Relay Security and Dependability Problems: A Case History, presented at the 29th Annual Western Protective Relay Conference, Spokane, Washington, 2002.

[10] DIGITAL COMMUNICATIONS FOR RELAY PROTECTION, Working Group H9 of the IEEE Power System Relaying Committee.

[11] G. Rosselli and K. Fodero "How to use Current Differential Relaying over Digital Phone Lines," Presented at the 31st Annual Western Protective Relay Conference, Spokane, Washington, 2004.

BIOGRAPHIES

Roy Moxley has a B.S. in Electrical Engineering from the University of Colorado. He joined Schweitzer Engineering Laboratories in 2000 as Market Manager for Transmission System Products. Prior to that he was with General Electric Company as a Relay Application Engineer, Transmission and Distribution (T&D) Field Application Engineer, and T&D Account Manager. He is a registered Professional Engineer in the State of Pennsylvania.

Ken Fodero is Research and Development Manager for the Schweitzer Engineering Laboratories, Inc., Pullman, Washington Transmission Engineering Division. Before coming to work at SEL he was a product manager at Pulsar Technology for four years in Coral Springs, Florida. At RFL Electronics he was Director of Product Planning for 15 years. He has also worked for Westinghouse Electric, now ABB, as Relay System Technician. Fodero is vice chairman of the Communications Subcommittee for IEEE PSRC. He graduated from RETS Technical School in New Jersey.

Back to Table of Contents

20040929
TP6174