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
roy_moxley@selinc.com and ken_fodero@selinc.com

SUMMARY

With more emphasis being placed on distribution system reliability, there is a need to establish protection methods for the varying communications in use on these systems. 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 their 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 is a prime qualitative measure for transmission relaying systems. Protection schemes 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. The scheme is selected to complement strengths or weaknesses of the communications.

HIGH-SPEED REQUIREMENTS FOR DISTRIBUTION SYSTEMS

End-user systems 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 a 13.8 kV line transmitting one of two feeds to a large industrial park (as shown in Figure 1). The distribution circuit could be two radial feeds from different sources or part of a distribution network similar to that described in Reference [3].

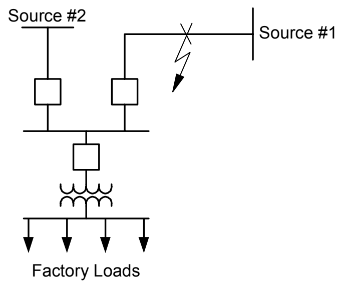

Figure 1: Factory Load With Two Independent Feeds

In a bulk power system, a fault near a transmission bus compromises the ability to transmit power across the entire system. In order to maintain system stability, clearing must be 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 online. 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, and the average restart time is 17 hours.

Distribution breakers 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 an instantaneous or time-overcurrent unit to operate in less than five cycles (80 ms), although such speed requires using the 0.5 time dial setting, with no coordination delay.

Figure 2 shows operating times of 34.5 kV overcurrent-based fault clearing at a large utility [5]. 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.

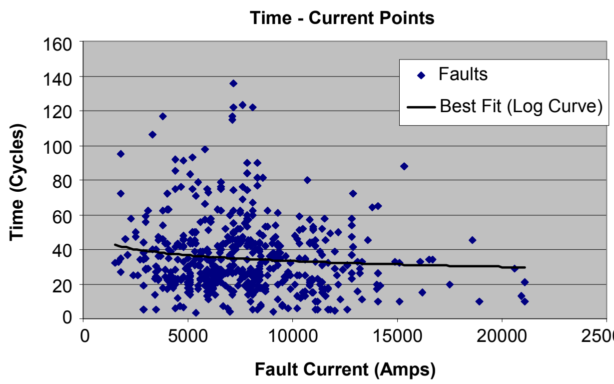

Figure 2: Typical Feeder Trip Time vs. Current

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.

COMMUNICATIONS NEEDED

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

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.

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

This paper will not examine microwave or power-line carrier for distribution protection. They are generally unsuitable for distribution systems because of cost or physical considerations.

DIRECT PILOT WIRE, LEASED DIRECT PHONE LINE

The protection applied when using a directly connected pilot wire or leased phone line is virtually always differential. In the same utility study referred to earlier [4], 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 wires being shorted, open, or reversed. This high failure rate clearly indicates that pilot wire monitoring is an essential part of any pilot wire protection system.

DIRECT CONNECTED FIBER

Point-to-point fiber optic has operational advantages, where it is available. For most distribution circuits, the cost of a dedicated fiber is prohibitive. 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.

MULTIPLEXED FIBER

While fiber-optic cable is immune from noise sources, the terminal and multiplexing equipment can produce noise or momentary loss of signal. As noted in Reference [7], a 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. Prior to the C37.94 interface, an unproven communications interface device was used. It provided 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 disable line protection on a regular basis.

RADIO SYSTEM

Even though optical fiber has operational advantages, 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 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. One check of a communication report from a relay connected to a radio system revealed the following (Table 2):

Table 2: Typical Radio Communication Report

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

This system 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 and proprietary synchronization methods between the transmit and receive ends that allow only a point-to-point connection. These radios use unlicensed frequencies, so 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 3). The time spent at any particular frequency is so short that interference causes only a short period of channel unavailability.

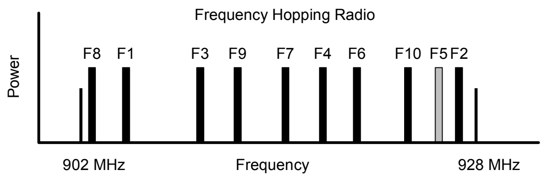

Figure 3: Interference to Spread-Spectrum Radios

Communications may be blocked while an interfering signal is present. Frequency Hopping Communications may be blocked only when a particular frequency collides with the interfering signal (F5 in Figure 3). 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 being sent within a particular band (Figure 4).

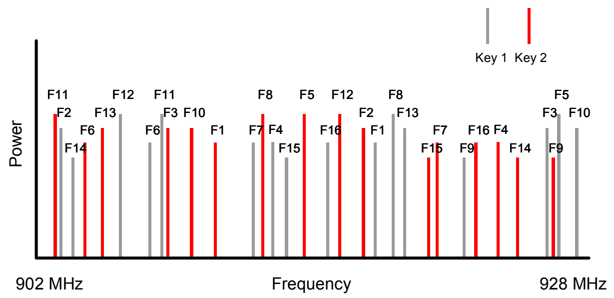

Figure 4: Avoid Interference By Changing Frequency Key

The change in availability over time is an illustration of this congestion effect. The following three reports were received from a utility in a major metropolitan area on a Friday, Saturday, and Sunday. 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	Unavail-ability
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				

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. 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.

A smaller metropolitan area installed radios for protection communications on two lines of 15 and 23 miles in length. 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.

Table 4: Small Community Spread-Spectrum Radio Unavailability

Dates	Total Failures	Relay Disabled	Longest Failure	Unavail-ability
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 measured, these systems are 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 like Table 5.

Previous tabulations of this type [7] are useful but have not included relative cost, speed, and other features. In distribution applications, cost considerations are very important.

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)	Medium (.00003)
Longest Failure (typical)	Very Long (days+)	Short	Very Short	Short (0.2 s)	Medium (20 s)	Short (1 s)
Fault-Related Failure Probability	High	Medium/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	Medium	Medium	High	High
Communication Speed (typical)	High (1–3 ms)	Medium (5–20 ms)	Very High (0.1 ms)	Medium (2–4 ms)	Med (2–4 ms)	Med (4 ms)
Data Rate	Very Low (4 kbps)	Medium (64 kbps)	Very High (4 gbps)	Medium (64 kbps +)	High (25 Mbps)	Medium (115.2 kbps)

PROTECTION SYSTEMS

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

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

Let us examine the three main schemes for their applicability to specific communications paths and distribution systems.

CURRENT DIFFERENTIAL

In the case of the utility referenced earlier [5], 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 5.

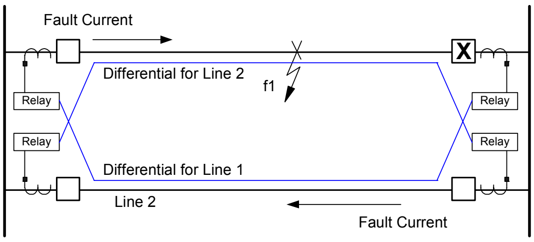

Figure 5: Power Lines and Communications

The communications frequently must be run either with the protected line or with a parallel line. Faults on the power line (f1) could disrupt communications.

One problem experienced 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 open a false trip. This experience 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 communication is not established as OK. This requires a “communications healthy” bit be a part of each message. The case described in Reference [6] shows the advantage of a system that does just this.

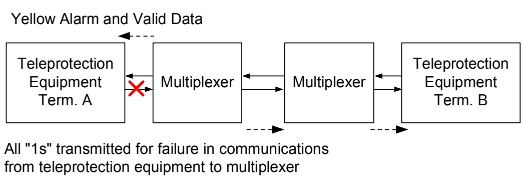

Figure 6: IEEE C37.94 Communication Standard

The diagram in Figure 6 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.

PERMISSIVE OVERREACHING TRANSFER TRIP (POTT)

A permissive tripping scheme provides a means to limit the protective zone of a relay scheme (Figure 7).

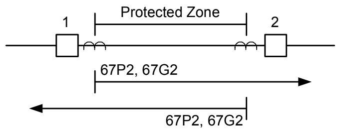

Figure 7: POTT Scheme Diagram

A permissive tripping protection scheme is biased to not operate 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 the case of distribution systems, protection is simplified 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, in Table 4 the longest outage was 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.

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 8).

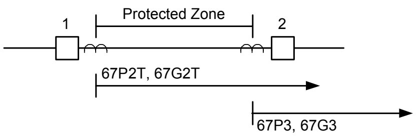

Figure 8: Directional Comparison Blocking (DCB) Scheme

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 sent only 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. Continuous monitoring of the channel is necessary to prevent false trips.

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 a protection scheme and communications system is 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 comms 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 [7]

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

[6] 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.

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

[8] 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.