Application of Digital Radio for Distribution Pilot Protection and Other Applications

Rich Hunt, Steel McCreery, Mark Adamiak **Al King**
GE Digital Energy

Networked distribution lines, sub-transmission lines, and industrial facility incoming supply lines have always presented an interesting protection challenge. As the number of distributed generators and cogeneration facilities increase, directional overcurrent protection and distance protection may not be selective enough for reliable protection without the implementation of pilot protection schemes such as permissive over-reaching transfer trip and directional comparison blocking.

Pilot-wire relaying has been the traditional solution at distribution voltages. Pilot-wire relaying sends a voltage signal between relays at each end of the line across copper wire. These voltages are used for differential protection. This scheme was used because of availability of copper pairs from the phone company and/or the low cost of installation of the communications wire. Today, however, copper pairs are no longer available from the phone company and the cost of installing new copper is increasingly expensive. When fiber access is available (typically at a premium cost), communication based digital protection solutions such as current differential relays and directional overcurrent relays in a pilot protection scheme are used.

The modern challenge is a method to provide digital communications for pilot protection that is reliable and affordable. Digital radio is an inexpensive method to provide digital communications for pilot protection at the distribution level. Digital radio has the ability to send permissive, blocking, and transfer trip signals over short to medium distances. Relay to relay messaging protocols have now become standardized through the IEC 61850 GOOSE profile and can provide not only protection information but also metering, monitoring, and control.

Practical concerns for the protection engineer include the reliability, security, and latency of digital radio communications, as this has a strong influence on selecting and setting the protection scheme. To address these concerns, this paper presents actual field data for radio signal reliability and latency. Based on this actual data, some recommendations for pilot protection schemes at the distribution level are presented. In addition, the paper also reviews the application requirements for digital radio, including design for redundancy, path concerns, antenna selection and site evaluation, and use of licensed and spread spectrum radios. Since modern digital radio also support higher communications bandwidth, the paper will explore some other innovative applications that can operate in concert with pilot protection communications.

1. Introduction

This paper considers the application of pilot protection on distribution lines. Pilot protection uses communications channels to send information between relays at each end, and is commonly used on networked lines. For the purpose of this paper we can assume distribution lines are circuits with an operating voltage typically between 4 KV and 69 KV. However, the principles discussed in this paper can be applied to any circuit at any voltage level, assuming the protection requirements for speed, security, and dependability can be met.

The protection challenges for pilot protection of distribution lines are identical to the protection challenges for pilot protection on transmission lines. The major goal for pilot protection is to operate dependably for a fault on the protected line and securely for faults outside the protected line (Figure 1). One challenge unique to distribution is that the protected line may change from a networked line to radial line quite frequently. If the line is from a utility source serving a load with generation capabilities, the line is only networked while the generation is running.

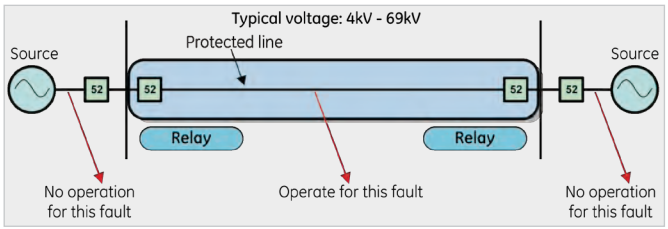

Figure 1.
Pilot protection challenge

2. Typical applications

The majority of distribution systems are radial systems, which allows the application of time-coordinated overcurrent protection schemes. While the overall distribution system may be designed as a radial system, individual pieces may be effectively networked. Short distribution lines to industrial facilities with significant generating capabilities, or short lines to independent power producers, may result in a small networked system. In addition, some parts of the distribution system are intentionally networked, such as in large urban load centers. In these cases, protection system must use a secure method of identifying faults to ensure appropriate isolation of faulted sections of the system. In any of these cases, some form of pilot protection is typically applied.

3.1 Industrial facility with fault current source

As mentioned above, one common example of an effectively networked radial distribution system is the short distribution line that connects an industrial facility with some generation to a utility distribution network. The local generation in the industrial facility may or may not be large enough to carry the complete facility load, but the generation is a source for short-circuit current on the incoming distribution line and the utility system. A less common example is an industrial facility with two different distribution feeds operating in parallel, where the second utility feed can provide short circuit current to the first utility feed. In either case, this application typically requires the use of some sort of directional protection, or protection that can identify the fault is on the incoming distribution line. There is only fault current contribution from the industrial facility when the local generation is running. The protection scheme must still operate correctly when the generation is not running and there is no contribution from the plant.

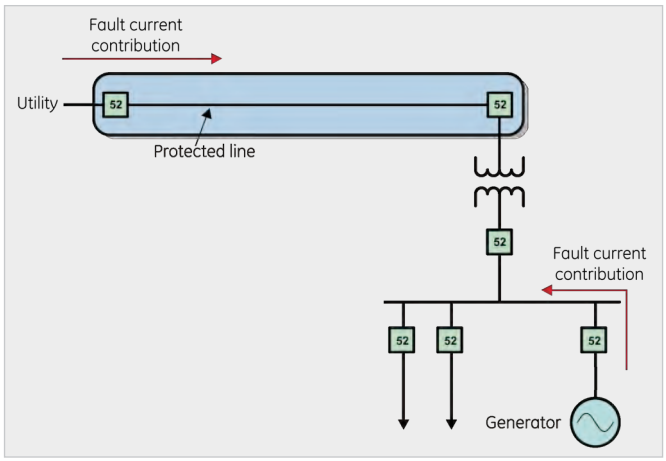

Figure 2.
Brick - rugged outdoor merging unit

3. Protection solutions

There are a variety of protection schemes for short, networked distribution lines. These schemes can be grouped as those requiring no communications between line terminals, and as pilot protection that requires communications between line terminals. The protection schemes that don't require communications use some form of directional protection, either directional overcurrent relays or distance protection. Just as with transmission line

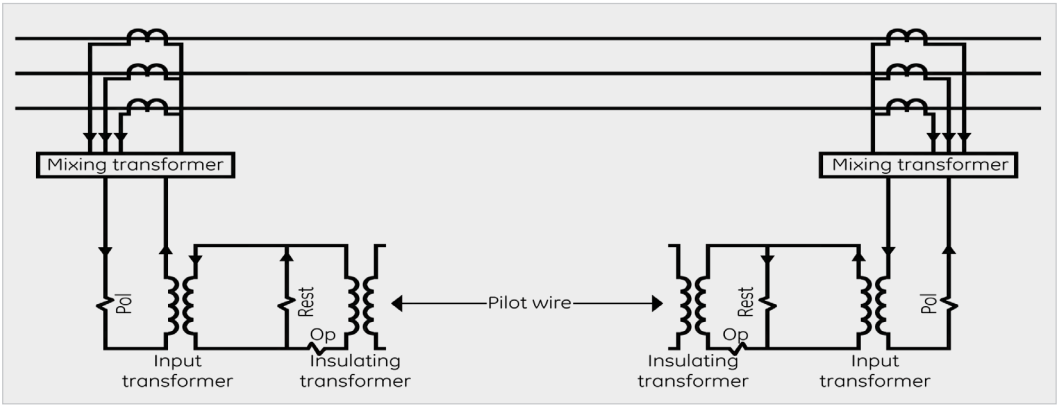

Figure 3.
Pilot-wire protection scheme

applications, directional protection is rarely applied on distribution systems without pilot communications in order to address concerns about coordination, security, and operating time.

Pilot protection schemes use some form of communications between relays at both line ends to ensure secure, selective tripping. The communications medium used depends on the type protection selected, the capabilities of the relay selected, and other factors such as cost of installation. Pilot protection methods may send analog values between relays at each end of the line, or they may use simple on/off, permissive, or blocking signals between relays at each end of a line.

3.1 Pilot-wire protection

One protection scheme that needs some emphasis is pilot-wire protection. Pilot-wire relays create a voltage signal to represent the measured current at the relay location. The pilot-wire relay then sends this voltage via telephone-type copper cable to the relay at the other end of the line. Pilot-wire relays use the voltages at each end in voltage differential protection. Pilot-wire relaying therefore requires only current measurements, is directionally secure, and is very simple to implement and set. Pilot-wire protection was the best solution from analog, electro-mechanical designs. For these reasons, pilot-wire protection has been the traditional solution for protection of short, networked distribution lines serving industrial facilities.

However, the industry is moving away from pilot-wire relaying as a solution for the protection of short, networked distribution lines. This move has little to do with the performance of pilot-wire relaying, but has more to do with the general trend towards digital relays and the use of digital communications. Once digital communications are used, current differential is a better protection choice. Digital representation of analog currents can be sent between each end, on a per-phase basis.

3.2 Other common protection methods

Other common protection methods for the short, networked distribution line include line differential relaying and pilot protection schemes such as permissive overreaching transfer trip (POTT) schemes and directional comparison blocking (DCB) schemes. All of these methods require communications between the relays at each end of the line. Line differential relaying generally requires a fiber-optic or other reliable communication channel. Pilot protection schemes require a communications channel that can transmit a binary, on/off, permissive or blocking signal. This channel can be a tone sent over an analog telephone line, power line carrier system, tone over microwave, or fiber-optic cable.

But the key piece of all of these protection methods, and a great challenge to reliability, is the communications channel. The communication channel must meet application requirements for performance, reliability, and cost. Performance requirements are clear: the communications channel must be physically capable of sending the correct type of pilot signal, have enough bandwidth to handle the signal, and have a short enough system latency time.

Reliability requires that the communications channel always be available. The channel consists of the actual media used, and any interface or conversion devices required between the relay and the communications channel. This is one of the reasons for the popularity of pilot-wire relaying. The connection between relays for pilot-wire relaying is a physical wiring connection, with no other devices to fail.

Cost of equipment, cost of installation, and cost of maintenance are all important considerations. For a new facility or expansion project, the cost of installing fiber-optic cable is only an incremental cost. However, as pilot-wire systems age, and the copper pilot wire degrades and fails, the cost of installation is a larger concern. Installing fiber-optic cable, or even copper cable, in a retrofit installation, is very expensive. The equipment costs may wind up as a trivial part of the total project cost.

Protection Method	Data Type	Message Size	Latency Time	Communications Media
Pilot-wire relaying	Analog (voltage)	-	< 1 ms	Metallic pilot-wire pair
Line differential relaying	Analog converted to digital message	Large	8 ms	Fiber-optic
Pilot protection (POTT, DCB)	Boolean (blocking signal, permissive signal)	Small	8-16 ms	Analog telephone line Microwave power line Carrier fiber-optic

Table 1.
Communications channel requirements

4. Digital Radio

The age of modern industrial radio data communications was ushered in when it was proven that digital data could be economically and reliably transmitted from one device to another using a voice radio set, known as narrow band radio, fitted with a modem. Packet radio is a term coined by amateur radio enthusiasts that refers to this type of digital radio communications equipment. Modern digital radios trace their design heritage back to the days of the first packet radios. Over the years technological advancements in the area of digital radio communications have led to a wide range of radio equipment for applications ranging from simple voice communications to the simultaneous transmission of multiple high-speed data channels over a wide band radio link.

The attraction of digital radio for protection of short distribution lines is installed cost, particularly in retrofit situations. For short lines (less than 1 mile in length) with good line of sight between line ends, the total equipment costs can be less than $5,000. The installation involves only a small project of around 16 to 24 man-hours for design and installation time. The concern over digital radios is performance. Performance of other communication medium and protection applications is well known and well understood by protection engineers. But digital radio is still new to the protection area. So the questions of performance related to data types, bandwidth, channel latency, distance, and reliability must be understood.

4.1 Data types

Currently at the physical layer digital radios apply two common interface standards: RS485 and 10BaseT Ethernet. The choice of interface directly impacts the transmission range and type of radio.

Interface	Protocol	Bandwidth	Type of Radio	Typical Maximum Distances
10BaseT	DNP3 via TCP/IP, ModBus, IEC 61850	0.5 MB	Spread spectrum: No License required	Up to approximately 20 miles (terrain permitting)
10BaseT	DNP3 via TCP/IP, ModBus, IEC6 1850	1.0 MB	Spread spectrum: No License required	Up to approximately 15 miles (terrain permitting)

Table 2.
Digital radio application guidelines

4.2 Terminology

Before proceeding further it is best to define some common terms that will be used through the rest of this application note.

Spread Spectrum Radios: Radio transmission using the spread spectrum technique was originally developed to provide jam-resistant military communications. Spread spectrum uses a modulation technique that distributes a transmitter's signal over a very wide bandwidth, making it virtually undetectable to a conventional radio receiver. Frequency Hopping spread spectrum and Direct Sequence spread spectrum are the two primarily methodologies spread spectrum technology uses to transmit messages today. Frequency Hopping spread spectrum radios are better in environments with interference, and are less likely to be jammed. Direct Sequence spread spectrum radios can support higher data bandwidths.

Narrow Band Radios: In communications, narrowband is a relative term. From one perspective these voice channel radios are the modern equivalent of the old packet radios. With baud rates of up to 9.6k they are typically used in SCADA applications supporting a single protocol such as DNP or ModBus. They are typically licensed with up to a 50 mile range.

Wide band: In communications, wideband is again a relative term. This term typically applies to radios that have a bandwidth of 200 KHz allowing multiple channels of data to be transmitted at the same time.

Access Point Radio: The radio that connects the remote radios together to form a wireless network. The wireless access point (WAP) usually connects to a wired network, and can relay data between the remote radios and devices on its wired network.

4.3 Digital radio performance testing

The best way to prove digital radio performance for pilot protection is to test performance under field conditions. The test in this case was for channel latency and channel reliability. The protection message between each relay is an IEC 61850 GOOSE message.

4.4 Application: Pilot protection via IEC 61850 GOOSE and spread spectrum radios

The radios were connected in a point-to-point topology, exactly as the typical pilot protection application. The test protocol was a simple matter of measuring the round trip time of each automatically generated IEC 61850 GOOSE messages transmitted from one relay to another relay and then immediately echoed back to the first relay.

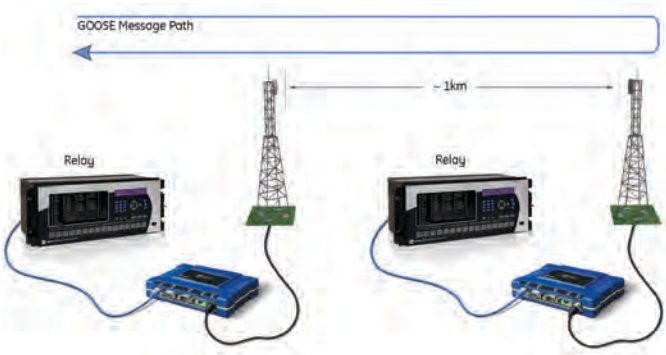

Figure 4.
Digital radio pilot protection test setup

This paper defines channel latency as the delay between the initiation of the GOOSE message by the sending relay and the reception of the GOOSE message by the receiving relay. The test actually measures the round-trip channel latency, as one relay measures the time between sending the original message and receiving the echoed response. Of interest for pilot protection applications is the one-way channel latency, which is assumed to be one half of this directly measured round-trip channel latency.

4.5 Performance

The test was actually a time-based test. The IEC 61850 GOOSE messages were sent back and forth for some length of time. At the end of the test, 29,672 messages were sent. The test results from the 29,672 consecutive messages are recorded in Table 3.

Round Trip Time	No. of Messages	Percentage
< 20 ms	232	0.78 %
20-30 ms	29.303	98.76 %
30-40 ms	127	0.43 %
40-80 ms	10	0.03 %

Table 3.
Radio performance test results

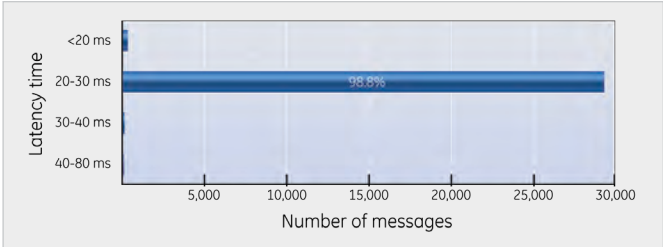

Figure 5.
Digital radio pilot protection test setup

The typical round-trip time is 20 to 30 ms, meaning the channel latency is 10 to 15 ms. This is very acceptable performance for pilot protection on distribution systems. Therefore digital radio meets general performance requirements for pilot protection applications.

4.6 Site installation and commissioning procedures

The key issue with any communications channel used for protection is the reliability of the channel, in this case specifically the reliability of the radio path. The important factors for digital radio are the distance between transmitter and receiver, obstructions in the line of sight between antennas, and the natural environment beneath the path.

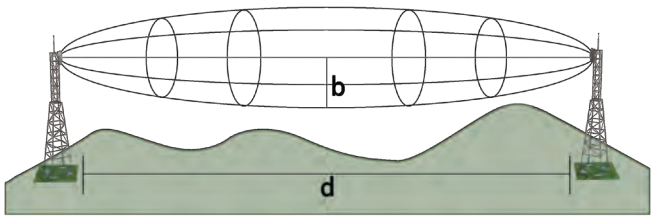

Figure 6.
Fresnel Zone

Radio communications is limited to "line of sight". However, radio line of sight is longer than the optical line of sight due to the bending of the radio wave towards the surface of the earth. This radio horizon is typically 30% longer than the visual horizon. Therefore, a longer communications path requires taller antennas to maintain the line of sight.

Obviously, obstructions in the line of sight will impact the performance of the digital radio, as the strongest radio signal is communicated directly along the radio line of sight. As obstructions block the width of the radio wave front, less of the signal gets through to the antennas. Obstructions may also cause multi-path interference due to reflective or refractive signals that may arrive at the receiver out of phase with the desired signal. However, due to the diffraction of the radio wave, objects not directly in the line of sight can also act as obstructions. The region where obstructions may impact the performance of the radio wave is known as the Fresnel zone.

DIGITAL RADIO IS AN INEXPENSIVE METHOD TO PROVIDE DIGITAL COMMUNICATIONS FOR PILOT PROTECTION AT THE DISTRIBUTION LEVEL

A Fresnel zone (Figure 6) is one of a (theoretically infinite) number of concentric ellipsoids of revolution that define volumes in the radiation pattern of the radio wave. There are multiple Fresnel zones, but only the first Fresnel zone is important for signal strength.

In practice, 60% of the first Fresnel zone must be clear of obstructions to allow successful radio communications. The radius of the Fresnel zone at its widest point (at the center of the radio line of sight) can be determined by:

$$b = 17.32\sqrt{\frac{d}{4f}}$$

Where b = radius of the Fresnel zone
d = distance between transmitter and receiver
f = frequency transmitted in GHZ

Beyond line of sight requirements and Fresnel zone requirements, the other concern with a digital radio path is fading, or the probability that the radio signal will be lost due to other conditions. The fade margin determines the allowable signal loss between the transmitter and receiver. The fade margin is a function of system gains (transmitter power, receiver sensitivity, and antenna gain) and system losses (free space loss, losses due to earth curvature, coaxial cable loss). Variations in the temperature and humidity of the atmosphere with elevation causes the signals to bend more or bend less, resulting in fading at the receiver. The longer the path, the more likely deep fades will occur, requiring a greater fade margin. The local propagation conditions impact the probability of signal fade as well. Generally, mountainous terrain is favorable, and tropical areas and those near large bodies of water are unfavorable.

One of the losses considered when determining the fade margin is free space loss. Free space loss is the loss in signal strength of the radio wave passing through free space. Free space loss is the basic path loss of the system. Free space loss is defined by:

Free Space Loss = 92.4 + 20 log(f) + 20 log(d) dB

Where f = frequency in GHz
d = distance in km

Like any other communications channel, proper installation results in desirable performance. The installation of digital radio systems requires proper site selection, an evaluation of path quality, and correct selection and mounting of antennas. The following is a brief overview of these requirements.

Evaluating Path Quality

For optimum radio performance, the installation sites for master and remote stations must be carefully considered. Suitable sites should provide:

- Protection of the radio equipment from direct weather exposure
- A source of adequate and stable primary power
- Suitable entrances for antenna
- Interface or other required cabling
- Antenna location that provides an unobstructed transmission path in the direction of the associated station(s).

Evaluating Path Quality

A line-of-sight path is ideal and provides the most reliable transmission in all cases. However, minor obstructions in the signal path will not necessarily block communication but will result in signal attenuation. In general, the need for a clear path becomes greater as operating frequency and transmission distance increases. Short-range paths (less than 1 mile) can be visually evaluated. Longer distances typically require a path study for new installations. A path study predicts the signal strength, reliability and fade margin of a proposed radio link. While terrain, elevation and distance are the major factors in this process, a path study must also consider antenna gain, feedline loss, transmitter power, and receiver sensitivity to arrive at a final prediction.

Antenna Selection and orientation

The single most important item affecting radio performance is the antenna system. Careful attention must be given to this part of an installation, or the performance of the entire system will be compromised. High quality, high gain antennas should be used at all master and remote stations. The antennas should be specifically designed for use at the intended frequency of operation.

Communication antennas are made by a number of manufacturers and fall into two general categories, omni-directional, and directional. An omni-directional antenna provides equal radiation and response in all directions and is therefore appropriate for use at master stations, which must communicate with an array of remote stations scattered in various directions. At remote stations, a directional antenna such as a yagi is typically used. Directional antennas confine the transmission and reception of signals to a relatively narrow lobe, allowing greater communication range, and reducing the chances of interference to and from other users outside the pattern. It is necessary to aim these antennas in the desired direction of communication. The end of the antenna (furthest from the support mast) should face the associated station. Final alignment of the antenna heading

can be accomplished by orienting it for maximum received signal strength. Most radio equipment includes provisions for measuring signal strength.

Antenna Mounting Considerations

The antenna manufacturer's installation instructions must be strictly followed for proper operation of a directional or omni-directional antenna. Using the proper mounting hardware and bracket ensures a secure mounting arrangement with no pattern distortion or de-tuning of the antenna. The following recommendations apply to all antenna installations:

- Mount the antenna in the clear, as far away as possible from obstructions such as buildings, metal objects, dense foliage, etc. Choose a location that provides a clear path in the direction of the associated station.
- Polarization of the antenna is important. Most systems use a vertically polarized omni-directional antenna at the master station. Therefore, the remote antennas must also be vertically polarized (elements perpendicular to the horizon). Cross-polarization between stations can cause a signal loss of 20 decibels (dB) or more.

Figure 7.
Omni-directional antenna

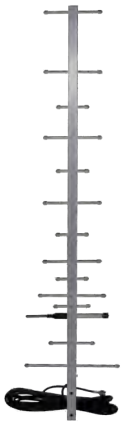

Figure 8.
Yagi antenna

The omni-directional antenna (Figure 7) is a typical antenna that used at an access point. The above Yagi antenna (Figure 8) is a typical antenna that would be use at a field station. Note the polarization this antenna is correct if used with either of the above omni-directional antennas.

Feedlines

The choice of feedline used with the antenna should be carefully considered.

Cable type	10 feet	50 feet	100 feet	500 feet
RG-214	0.76 dB	3.8 dB	7.6 dB	Unacceptable Loss
LMR-400	0.39 dB	1.95 dB	3.90 dB	Unacceptable loss
½ inch HELIAX	0.23 dB	1.15 dB	2.29 dB	11.45 dB
7/8 inch HELIAX	0.13 dB	0.64 dB	1.28 dB	6.40 dB
1-1/4 inch HELIAX	0.10 dB	0.48 dB	0.95 dB	4.75 dB
1-5/8 inch HELIAX	0.08 dB	0.40 dB	0.80 dB	4.00 dB

Table 4.
Feedline signal loss

Poor-quality coaxial cables should be avoided, as they will degrade system performance for both transmission and reception. The cable should be kept as short as possible to minimize signal loss. For cable runs of less than 20 feet (6 meters), or for short range transmission, an inexpensive type such as Type RG-8A/U may be acceptable. Otherwise, use a low-loss cable type suited for 900 MHz, such as Heliax®.

Setting the output power

The maximum transmitter output power allowed under FCC rules is +30 dBm. The power must be decreased from this level if the antenna system gain exceeds 6 dBi. The allowable level is dependent on the antenna gain, feedline loss, and the transmitter output power setting.

NOTE: In some countries, the maximum allowable transmitter output may be limited to less than the figures referenced here. Be sure to check for and comply with local requirements.

Example:

To determine the maximum allowable power setting of the radio, perform the following steps:

1. Determine the antenna system gain by subtracting the feedline loss (in dB) from the antenna gain (in dBi). For example, if the antenna gain is 9.5 dBi, and the feedline loss is 1.5 dB, the antenna system gain would be 8 dB. (If the antenna system gain is 6 dB or less, no power adjustment is required.)

2. Subtract the antenna system gain from 36 dBm. The result indicates the maximum transmitter power (in dBm) allowed under the rules. In the example above, this is 28 dBm.

SWR of the antenna system

A proper impedance match between the transceiver and the antenna system is very important. It ensures the maximum signal transfer between the radio and antenna. The impedance match can be checked by measuring the SWR (standing-wave ratio) of the antenna system. The reflected power should be less than 10% of the forward power (≈2:1 SWR). Higher readings usually indicate problems with the antenna, feedline or coaxial connectors. If the results are normal, record them for comparison for use during future routine preventative maintenance. Abnormal readings indicate possible trouble with the antenna or the transmission line that will need to be corrected.

4.7 Digital radio and security

One concern with digital radio is communications security. Traditional communications channels for protection are physically isolated from computer networks, and therefore carry little security risk. However, digital radio signals are theoretically available to anyone with the proper equipment. Security issues fall into the categories of protection of privacy, protection from unauthorized access, and protection from denial of service attacks.

Protection of privacy

Unlicensed spread spectrum radios, such as those suggested for pilot protection in this paper, are inherently secure. Spread spectrum technology was developed during World War II for the military due to its ability to reject jamming and the difficulty in intercepting transmission. The tools available to hackers to

intercept radio frequency messages are designed for WiFi signals. WiFi is a different communications standard than that used by digital radio, and these tools will not intercept digital radio signals.

The only practical way to intercept messages is with a stolen radio. However, all software that operates the radio resides within the radio. This prevents common hacker tricks such as putting stolen wireless cards in promiscuous mode. It's difficult to therefore actually retrieve and read the messages using just a stolen radio.

In addition, digital radios support AES-128 or RC4 encryption standards. Both AES-128 and RC4 encryption use a key. This key is required to decrypt the data. Unlike earlier encryption technology the key isn't static in that it is rotated with other keys after a short period of operation. So access to the radio still doesn't result in access to data.

THE ATTRACTION OF DIGITAL RADIO FOR PROTECTION OF SHORT DISTRIBUTION LINES IS INSTALLED COST, PARTICULARLY IN RETROFIT SITUATIONS

Protection from unauthorized access

This next level of security assumes that a hacker is already connected to the network using a stolen radio (This is a big assumption). To prevent a break-ins authentication is used to allow the radio access to the network. There are several standards revolving around authentication. For standard IT equipment such as routers, switches, and WIFI the authentication standard that applies is called 802.1x RADIUS authentication. When larger organizations implement authentication it will be 802.1x RADIUS. Digital radios can comply with 802.1x RADIUS. The same radios will also work without 802.1x RADIUS and have local authentication that will provide the user with a high level of security.

Protection from denial of service attacks

There are many different attacks. One for example would be to redirect traffic. The predominant strategy against denial of service attacks is to prevent unauthorized people from configuring the radios. To protect against dictionary attacks, which a hacker may try to break the password, radios have a feature were after three login failures, the transceiver ignores login requests for some period of time.

Digital radios can become part of a company's regular IT network. Unprotected access points on the network provide access to any connected radios. For this reason, organizations may insist upon implementing remote login to network managed devices with SSH management or HTTPS. The SSH or HTTPS management standard is basically an encrypted telnet for IT equipment configuration. This prevents someone monitoring the network to use an unsecured access point from seeing the data within the telnet session.

In addition, digital radios are compliant with SNMP version 3 which may be implemented on larger systems. SNMP version3 or Simple Network Management Protocol Version 3 (SNMPv3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to managed devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are:

- Message integrity—Ensuring that a packet has not been tampered with in-transit.
- Authentication—Determining the message is from a valid source.
- Encryption—Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

5. Digital Radio Pilot Performance Comparison

With end-to-end performance in the 10 - 15ms range, digital radio immediately places itself in the mix of usable pilot channels in the protection and control world. Traditional pilot protection channels include Power Line Carrier, Audio Tone, and more recently digital channels via fiber (direct or multiplexed) or copper. Although not quite as fast as the total time of direct fiber or a wide-band carrier set (3.5 – 6 ms), it compares quite favorably to analog tone over an analog microwave (13 – 18ms) or a digital channel through a modem (15-18ms).

This paper explicitly discusses the use of an IEC 61850 GOOSE message transmitted over Ethernet. One reason is that Ethernet radios are an inexpensive, easy to configure solution for digital radio applications. In addition IEC 61850 is a non-proprietary solution, as the GOOSE is an international standard with demonstrated multi-vendor interoperability. The GOOSE is configurable to communicate multiple Status, Analog Values, and Quality values in a single message. The 10 – 15 ms message delivery time mentioned above is invariant for GOOSE packets containing limited combinations of the above data items. Also, using an IEC 61850 GOOSE message over Ethernet provides impressive error checking capabilities to ensure messages are correctly received. The radios use a 16-bit CRC, and the GOOSE message uses a 32-bit CRC. This larger CRC eliminates the need for security counts on received messages for permissive or blocking signals. If the CRC is validated, there is only a 1 in 4 billion chance that the received message is incorrect. Also, digital radios using Ethernet can support other communications traffic than simply protection. By using a VLAN, protection GOOSE messages will always have priority over other types of traffic, so no channel delays occur.

There are other methods to implement digital radio as a pilot protection communications channel. One possibility is to use radios that transmit physical contact closure states, similar to traditional power line carrier or microwave solutions. Another possibility is to use a proprietary pilot protection communications protocol available from various relay vendors. This method requires relays from the same vendor on each end of the line, and requires the radios can actually transmit this proprietary protocol. Depending on the method selected (contact closure or protocol), the radios selected, and the actual protocol used, the channel latency can be significantly less than that of IEC 61850 GOOSE messages over Ethernet. These methods may only work

with specific models of radios, and may require the use of radios operating on licensed transmission frequencies. These methods will not use the 32-bit CRC error checking available through IEC 61850 GOOSE messaging, and may not implement the 16-bit CRC available in Ethernet-enabled digital radios.

A challenge for any radio system is interference. Interference can come from paging transmitters, co-located transmitters, receiver overload, and rectification in metal structures. The issues around interference are usually site specific, as are the solutions to eliminate interference. One common solution, especially when multiple radio transmitters are present, is to cross-polarize antennas. Most systems use vertical antenna polarization. Cross-polarizing by going to horizontal polarization in one system reduces on-channel or adjacent-channel interference by about 20 dB. Power system faults are not a concern, however. The majority of the energy for a power line fault is centered on a 10 MHZ bandwidth, and doesn't exceed 100 MHz. Spread spectrum radios operate at 900 MHZ, well above this bandwidth.

6. Pilot Protection with digital radio

Although latency through the digital radio may be a concern, when operating in the distribution realm, a system latency of 10 –15 ms is typically acceptable. A second concern may be the need for redundancy in case the radio communications fail for some reason. These are similar concerns to pilot protection for transmission line applications.

The best way to discuss these performance criteria is to look at specific examples of pilot protection using digital radio as applied to the distribution feeder supplying an industrial facility. Specifically, we'll discuss a POTT scheme, a DCB scheme, a reverse interlocking scheme, and any combination POTT/DCB scheme. This paper assumes that all protection scheme logic is performed with a microprocessor-based relay. Obviously, traditional hardwire control logic can be used as well. It is important to note that the microprocessor-based relay treats the GOOSE message the same as any other digital input. The status of the specific bit from the GOOSE message is utilized in the relay logic just the same as a regular contact input.

6.1 POTT scheme

This application of the POTT scheme (Figure 9) uses definite time directional overcurrent or distance elements. These definite time directional overcurrent elements are set to see faults beyond the other end of the line, and are configured with no intentional time delay. Instantaneous tripping is acceptable, because a permissive signal from the other end of the line is required to allow tripping. Since the relays at both ends must send a permissive signal for the POTT scheme to operate, there must be a source of the fault current for the protected line at each end of the line. Depending on the capabilities of the relay used for the POTT scheme, it may be possible to implement a weak infeed/echo logic to account for no source on one end.

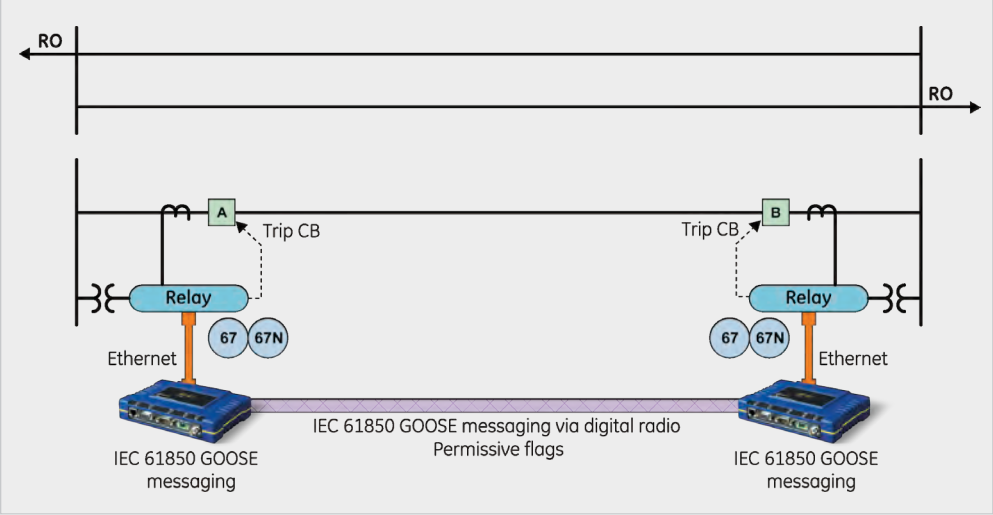

Figure 9.
POTT scheme using digital radio

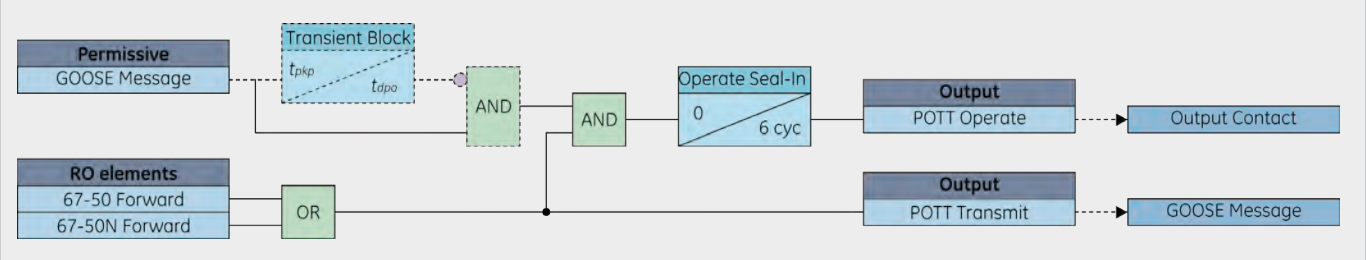

Figure 10.
POTT scheme logic

The internal relay logic for the POTT scheme is actually quite simple. When either the phase or neutral directional overcurrent element picks up, a GOOSE message containing a permissive flag is sent to the relay on the other end. If a GOOSE message containing a permissive flag is received from the other end while either of the local overcurrent elements is picked up, the relay trips the local circuit breaker. There is no intentional time delay in this scheme. For a fault on the protected line, the total operating time of this scheme will be approximately 30 to 35 ms, ignoring the breaker operating time. This assumes a channel latency of 10 to 15 ms, and approximately 20 ms for the relay element to operate.

Traditional POTT schemes (Figure 10) using analog communications such as power line carrier or microwave use a pickup time delay on the permissive receive signal in case of spurious signal reception. Since this implementation uses a digital status contained in a GOOSE message, there is no need to add this pickup time delay. There is no need to add a pickup time delay to the permissive receive signal, as this is a digital status contained in the GOOSE message. Also, there is no need to add a security count to the permissive receive signal. Validation through the 32-bit CRC of the GOOSE message ensures the received message is correct. For this simple, one line application, there is no need to add any transient blocking delay for current reversal. However, if parallel lines are serving the same facility or tied to the same bus, then a transient blocking delay for current reversal must be added on to the permissive receive signal.

6.2 DCB scheme

The DCB scheme (Figure 11) also assumes the use of definite time directional overcurrent or distance elements. The DCB scheme requires a forward directional overcurrent or distance element looking towards the protected line for tripping, and a reverse directional overcurrent or distance element looking behind the protected line to initiate a blocking signal. The reverse directional overcurrent or distance element that initiates the blocking signal is set with no intentional time delay.

The directional overcurrent or distance element that is used for tripping is set with a short time delay to account for channel delay time. This time delay can be set to approximately 4 cycles to allow for the maximum message latency of 40 ms plus approximately 1 cycle for the remote relay to initiate the blocking signal. Therefore, the total operating time for protection of the line will be 4 cycles, ignoring breaker operating time.

It may be necessary to add a short seal-in timer to hold the blocking signal (Figure 12). The blocking signal is a digital flag contained in a GOOSE message. Since the loss of one GOOSE message will cause the blocking signal to drop out, this timer ensures the blocking signal is maintained when an individual message is lost. Assuming that the blocking GOOSE message is sent in 4 ms, a 1-cycle time delay means that four consecutive GOOSE messages must be

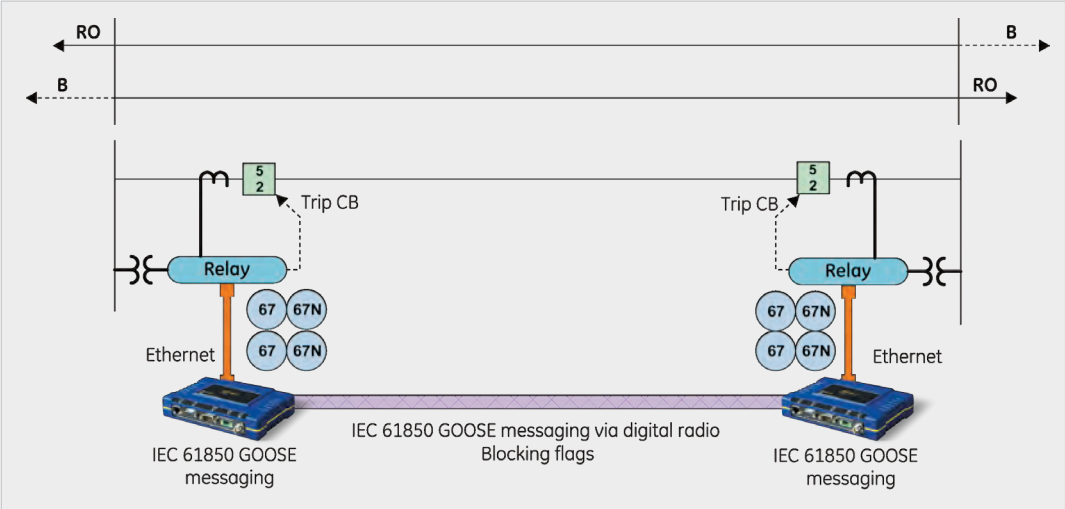

Figure 11.
DCB scheme using digital radio

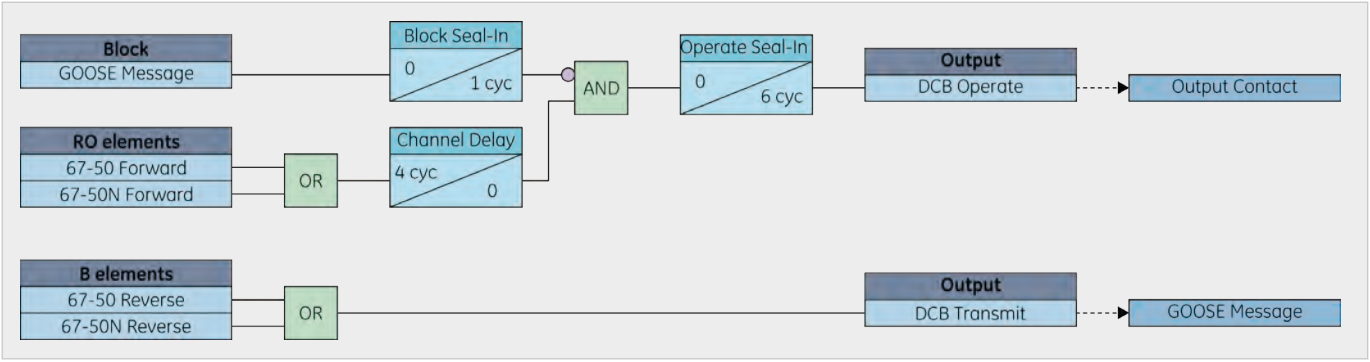

Figure 12.
DCB scheme logic

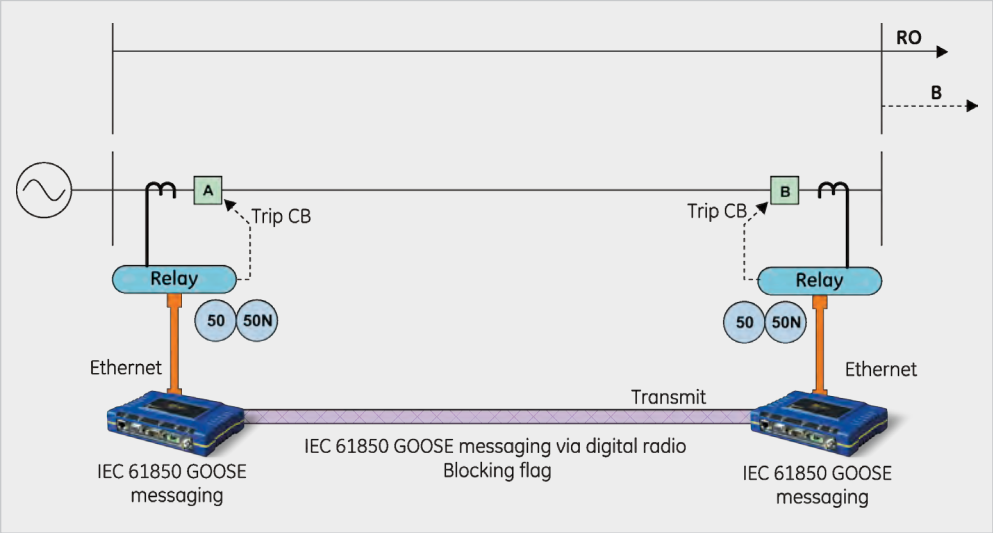

Figure 13.
Reverse interlocking scheme using digital radio

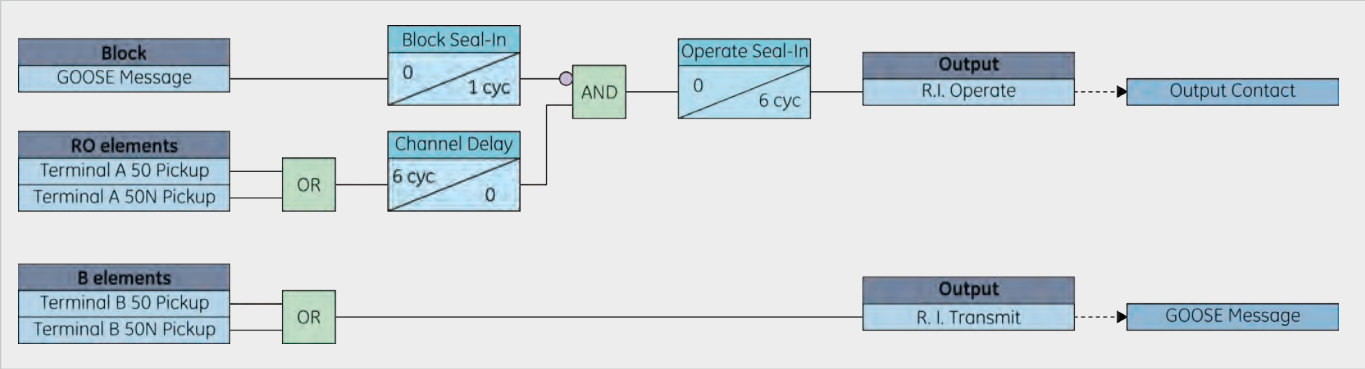

Figure 14.
Reverse interlocking scheme logic

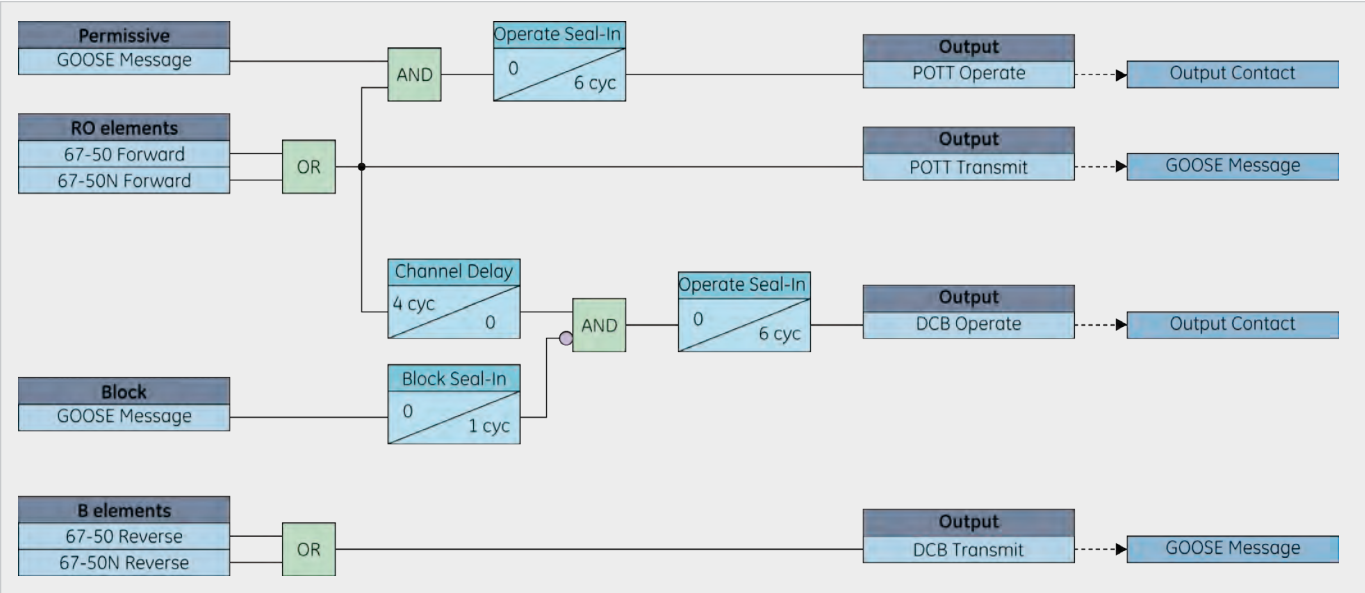

Figure 15.
POTT/DCB combination scheme logic

lost before the block is released. The 1 cycle time delay also means the blocking signal must drop out for one cycle before tripping is permitted.

6.3 Reverse interlocking scheme

Even when the distribution feeder for a large load or industrial facility is a radial feed, it may be desirable to it implement pilot protection on the incoming distribution feeder. Pilot protection should result in faster clearing times for faults, and alleviate many coordination issues. Pilot protection in this instance can be a simple reverse interlocking protection scheme (Figure 13). In a reverse interlocking scheme, both downstream and upstream relays use high-speed overcurrent protection. When the downstream relay picks up for a fault, this relay sends a blocking signal to the upstream relay. The overcurrent element on the downstream relay is set to overreach the downstream line end, and with no intentional time delay. The overcurrent element on the upstream relay is set with a short time delay of 4 to 6 cycles. The short time delay allows the downstream relay detect the fault and initiate the locking signal, and this time delay allows for maximum latency (40ms) of the digital radio message.

The logic for the reverse interlocking scheme (Figure 14) is different in the relays at the source end and the load end of the line. The relay at the load end of the line, Terminal B in this example, simply sends a blocking signal when an overcurrent element picks up. The relay at the source end of the line, Terminal A in this example, can only operate when overcurrent elements are picked up and no blocking signal is received from the relays at Terminal A. Reverse interlocking is in some ways a simpler form of the DCB scheme. The operating time is similar, but with the total clearing time for a fault of the protected line of approximately 6 cycles, ignoring breaker operating time.

IEC 61850 GOOSE MESSAGES OVER ETHERNET PROVIDES IMPRESSIVE ERROR CHECKING CAPABILITIES TO ENSURE MESSAGES ARE CORRECTLY RECEIVED

6.4 Combination of POTT/ DCB scheme

For increased reliability, one possibility is to apply both the POTT scheme and a DCB scheme operating in parallel. The POTT scheme should operate essentially instantaneously for fault on the protected line. The DCB scheme, due to the need to initiate and receive a blocking signal, has a short time delay of 4 to 6 cycles. Therefore, for an internal fault, but POTT logic should trip instantaneously. If the fault fails to clear, such as for a breaker failure condition, the DCB logic will trip in 6 cycles. Consider the fault conditions if the digital radio fails. For a fault on the protected line, the POTT logic will not operate because no permissive signal is sent or received. The DCB logic will operate, as no blocking signal is sent or received. For a fault not on the protected line, once again the POTT logic will not operate. However, the DCB logic will operate, as no blocking signal is received or sent. It may be desirable to increase the time delay of the DCB logic to allow other protection to clear external faults.

This combination scheme (Figure 15) is very attractive when the line being protected is the line to an industrial facility with generation. When the facility generation is running, both the POTT and the DCB scheme will operate correctly. However, when the generation is not running, the POTT scheme will not operate correctly for fault on the protected line. The directional overcurrent relay at the plant end of the line will not see a fault on the protected line, and will therefore not send a permissive signal. However, the DCB scheme will operate correctly in this case. No blocking signal will be sent when the fault is on the protected line. However, for a fault in the plant itself, a blocking signal will be sent to the utility end of the line.

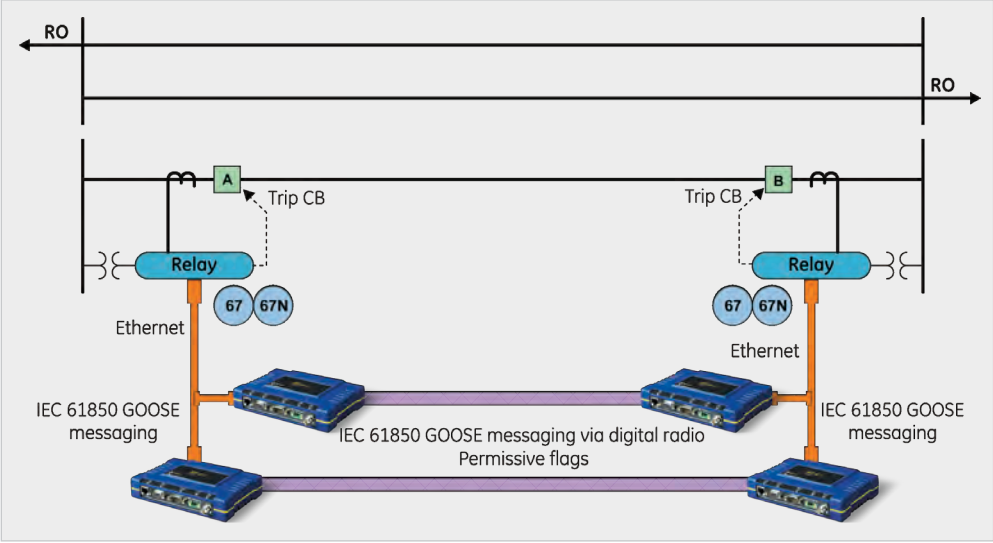

Figure 16.
POTT/DCB combination scheme logic

6.5 Scheme Considerations

These examples show that digital radio using IEC 61850 GOOSE messages can be the communications channel for the two most common pilot protection schemes. By extension, digital radio can be used in any pilot protection scheme, including Directional Comparison Unblocking (DCU), Permissive Underreaching Transfer Trip (PUTT), and the Hybrid POTT scheme. This paper uses the POTT and DCB schemes as examples to show that digital radio can perform in both a permissive logic and a blocking logic.

The POTT scheme is a very secure scheme, but will fail to operate on a loss of communications channel during an in-zone fault. The DCB scheme is a very dependable scheme, but may operated incorrectly for an out-of-zone fault during a loss of communications channel. These risks have always existed, starting with power line carrier communications. In fact, the DCU scheme using frequency shift keying is a scheme designed around the unreliability of the power line carrier signal. The correct choice of pilot protection scheme when using digital radio is therefore part of the art and science of protective relaying. Philosophy, experience, and application criteria will lead to the best solution for a specific situation.

6.6 Redundancy considerations

As with any other protection scheme, there are redundancy and backup considerations when using digital radio as part of a pilot protection scheme. The previous application of a combination POTT and DCB scheme is one such example of redundancy. If for any reason the digital radio channel fails, the line will still trip for internal faults. However, there could be a loss of security for external faults. A simple way to add redundancy is to use two separate radio paths for communications. In other words, simply use 2 separate radio sets. The same GOOSE message is sent to each radio, and both GOOSE messages are received by the relay. That way, if one set of radios fails to communicate, the other set will still operate. This method requires one of the radio sets to use cross-polarized antennas to prevent channel interference.

7. Other Applications

7.1 Other protection applications

Obviously, pilot connection using digital radio can be applied in any network distribution line application including a line serving IPPs, and networked distribution lines downtown load centers. However, when the digital radio used is an Ethernet-based radio, the radio essentially establishes an Ethernet network between remote devices. This allows the extension of the protection scheme in interesting ways.

Parallel feeders

Parallel feeders from a utility serve some industrial facilities. In this case, separate pilot protection systems are required for each incoming distribution line. However, with digital radio, one set of radios can be the communication channel for multiple sets of lines. Each relay simply sends a GOOSE message to the radio, or receives a GOOSE message from the radio, as appropriate. Using two sets of radios in this case provides complete reliability of communications. Each pilot protection system sends its tripping or blocking signals over both sets of radios. Therefore both lines have a primary and secondary communications channel while requiring only two sets of radios. To extend this example even further, consider a plant that has three incoming utility feeds. Two sets of radios provide a redundant communications path for all three incoming feeders.

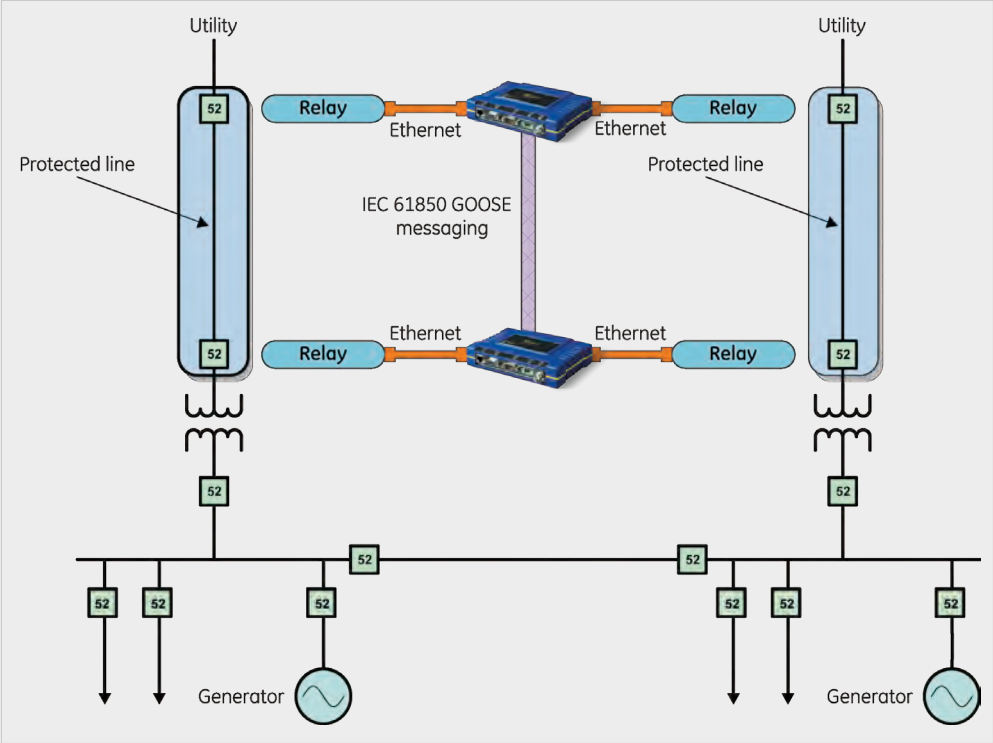

Figure 17.
Parallel feeder application

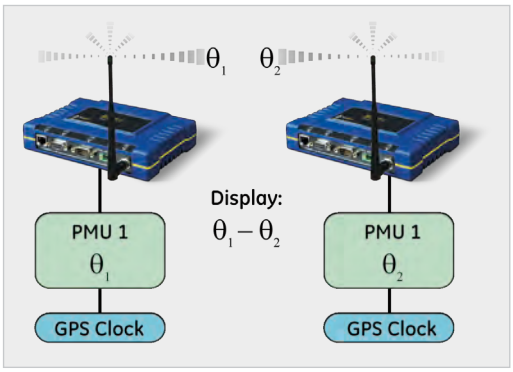

Figure 18.
Mobile phase angle verification system

7.2 Other Digital Radio Channel Applications

Given a digital communication channel in a substation, a wide variety of ancillary functions become available. When using a digital radio channel in an application, the channel is available 99.9% of the time for other applications. In the case of an Ethernet-based radio, the Ethernet can be connected to all other devices in the remote substation and provide complete data access. This access would typically include SCADA (with remote control), remote setting/SW updates, oscillography and Sequence of Events retrieval, and physical security monitoring.

Besides the typical substation functions mentioned above, digital connectivity enables the ability to transmit digital images. Specifically, many remote control functions require visual confirmation of an operation such as the opening of a disconnect. By providing a position-selectable camera, an operator can position the camera to focus on a substation device (e.g. – switch), visually check the status of the device before the control operation, execute the control operation, and then verify the result of the operation.

Another recently field-tested application had to do with mobile verification of the angle reference of distribution feeders. In this application, there was an operational need to be able to verify the phasing between a substation source and the service in a customer location. The distance between the substation and the customer premises could range from dozen's of meters to 2km. The solution of this mobile monitoring application was the use of a set of Phasor Measurement Units (PMU) – synchronized by a set of GPS clocks – and communicating with GOOSE through Ethernet digital radios. Each PMU measured the absolute local angle (either the source angle or the customer's service angle) and each end then communicated the measured angle to the other via GOOSE. The received angle was subtracted from the locally measured absolute angle and the relative difference was then displayed. This system is illustrated in Figure 18.

8. Summary

This paper describes basic digital radio technology and shows some possible applications of digital radio for distribution protection. As with any other pieces of the protection system, it is important to understand the reliability and performance of digital radio. The test results documented in this paper show that digital radio successfully sends an IEC 61850 GOOSE message within 10 to 15 ms 99% of the time. In no case during the test was a message not received. Therefore digital radio is reliable enough to use as part the distribution protection system. The 10 to 15 ms channel latency is more than acceptable for distribution protection, is interoperable, and requires no special adaptation of standard pilot protection schemes. The channel latency compares quite favorably to that of analog tone over an analog microwave, or a digital channel through a modem, meaning that digital radio is appropriate for pilot protection communication on sub-transmission lines.

Advantages of digital radio in being able to establishes an Ethernet network was presented. Additionally, digital radios support any standard protocol over Ethernet, including Modbus, DNP 3.0, and IEC 61850. At a minimum, this allows digital radio to send the binary signals necessary for pilot protection, such as permissive and blocking signals. In addition, digital radio, like any other Ethernet network, allows simultaneous traffic. Therefore digital radio can support communications for pilot protection, SCADA communications, and metering communications simultaneously without any degradation in performance.

When one looks at the capabilities of digital radio, and the low installed cost of digital radio, many interesting applications present themselves.

9. References

[1] J. L. Blackburn, "Protective Relaying Principles and Applications", 2nd edition, Marcel Dekker, Inc., New York, NY, 1998.

[2] J. R. Fairman, K. Zimmeramn, J. W. Gregory, J. K. Niemira, "International Drive Distribution Automation and Protection", 27th Annual Western Protective Relay Conference, Spokane, WA, October 24th – 26th, 2000.

[3] "IEEE Guide for Protective Relay Applications to Transmission Lines", IEEE Std. C37.113-1999, The Institute of Electrical and Electronic Engineers, Inc., New York, NY, 2000.

9. Symbols

Symbol	Definition
	Current source
52	Circuit Breaker
Relay	Digital Relay
Radio	Digital Radio
67 67N	Directional Overcurrent (Phase and Neutral)
RO	Overreaching protection element
B	Blocking protection element
AND	Logical AND
OR	Logical OR
Timer t t	Timer element
	Ethernet connection

041310-v4