Speed and Security Considerations for Protection Channels

Shankar V. Achanta, Ryan Bradetich, and Ken Fodero
Schweitzer Engineering Laboratories, Inc.

This paper was presented at the 69th Annual Conference for Protective Relay Engineers and can be accessed at: https://doi.org/10.1109/CPRE.2016.7914917.

For the complete history of this paper, refer to the next page.

Published in
Sensible Cybersecurity for Power Systems: A Collection of Technical Papers Representing Modern Solutions, 2018

Previously presented at the
69th Annual Conference for Protective Relay Engineers, April 2016

Originally presented at the
42nd Annual Western Protective Relay Conference, October 2015

Speed and Security Considerations for Protection Channels

Shankar V. Achanta, Ryan Bradetich, and Ken Fodero, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Communications play a vital role in the fast and reliable operation of protection systems. Advances in communications technologies have enabled utilities to improve the speed, security, and dependability of these systems. Communications-based protection schemes have employed power line carrier (PLC), microwave, fiber-optic communications, time-division multiplexing, Ethernet, and spread-spectrum radio systems. Each communications transport system must provide low latency and be deterministic, secure, and dependable. Pilot protection schemes are not one size fits all. The clearing time requirements for a protected line or a breaker failure transfer tripping scheme can vary based on loading and system stability requirements.**

This paper describes the communications requirements for various protection and control applications, including channel time, channel asymmetry requirements, and jitter. We discuss the advantages and disadvantages of communications technologies, including PLC, microwave, fiber optics, synchronous optical networks, and spread-spectrum radios. We describe how network topologies can improve security and dependability. We also discuss cybersecurity practices that are suitable for securing protection communications links.

I. Introduction

There are many communications options available today for relay pilot protection schemes. These schemes have been developed and refined over many years to take advantage of the strengths of the various communications media and technologies, while providing logic that supplements the weaknesses of each specific communications system. This paper explains the performance requirements for the various communications systems and which pilot protection schemes match these requirements based on the communications system performance. For this paper, we define a pilot protection scheme as the combination of the protective relay (along with its logic) and the communications device providing the line protection or transfer tripping. The communications devices that provide the relay interface are referred to as teleprotection devices.

II. Speed and Security

The total operation time of a pilot protection communications scheme as well as the security and dependability of the commands sent are the key measures of performance for pilot protection systems.

Security is a measure of the teleprotection system's immunity to misinterpreting noise or corrupted data as valid commands and issuing invalid outputs. For analog-based communications systems, such as power line carrier (PLC), security is measured by the number of noise bursts at various signal-to-noise ratios (SNRs) that are required to produce a false command output. The results are then plotted to provide a security performance curve. Fig. 1 is an example security curve from ANSI C93.5 [1]. This standard defines the method to test and document the security of a PLC system.

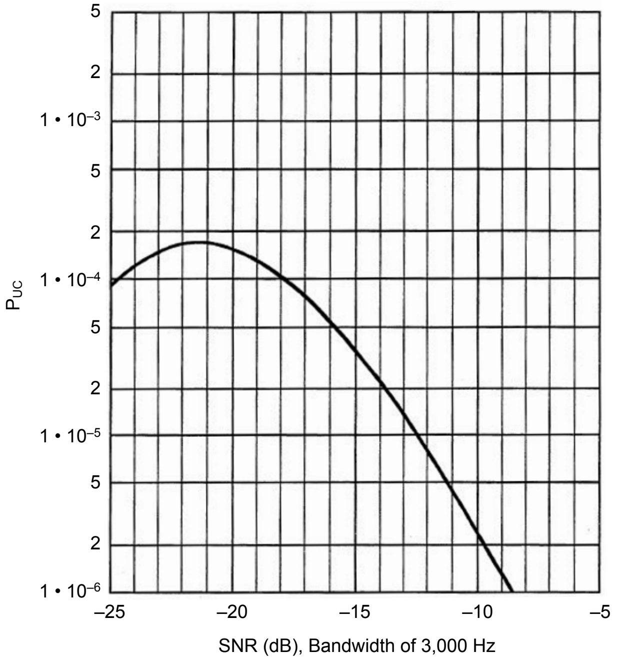

Fig. 1. Example security curve from ANSI C93.5

For digital pilot protection communications systems, including line current differential (87L) protection, security can be measured as defined in IEC 60834-1 [2]. This standard defines security as 1 – P_{UC}, where P_{UC} is the probability of an unwanted command. The estimate of P_{UC} can be stated as follows:

$$P_{UC} \approx \frac{N_{UC}}{P_B} \quad (1)$$

where:

N_{UC} is the number of unwanted commands.

P_B is the number of noise bursts applied.

Dependability is a measure of the system's ability to produce a command output during the presence of channel noise or communications disruptions. IEC 60834-1 states that dependability versus SNR should be measured by comparing the number of commands delivered to the receiver within an acceptable actual transmission time with the number of commands sent from the transmitter.

The estimated probability of missing a command (P_{MC}) is stated as follows:

$$P_{MC} \approx \frac{N_T - N_R}{N_T} = 1 - \frac{N_R}{N_T} \qquad (2)$$

where:

N_T is the number of commands sent.

N_R is the number of commands received.

The dependability is then given by 1 – P_{MC}.

Security, dependability, and speed tend to interact. For example, efforts taken to increase security typically adversely affect dependability and vice versa. Reducing the speed (at the teleprotection device) has an adverse effect on security. Many of the pilot protection schemes and equipment used today have maximized this balance and have predetermined settings that can be used to vary security, dependability, and speed.

III. Communications-Based Protection Schemes

Teleprotection and relay-to-relay protection communications evolved from audio tone to synchronous 64 kbps data and lower speed asynchronous data communications. These data formats allow us to take advantage of the increased speed and performance that come with the dedicated fiber and private time-division multiplexing (TDM) networks available for protection. Protection communications scheme latencies evolved from 8 to 12 ms typical of analog circuits to 3 to 5 ms. Today, almost all line current differential and teleprotection systems have been designed for use over TDM circuits.

Teleprotection devices use communications channels to compare information from the line terminals and provide high-speed fault clearing for 100 percent of the protected line. High-speed clearing of faults along the entire line segment is required or desirable for several reasons.

A short circuit on a power system reduces the ability of the power system to transfer power. Reducing the short-circuit duration on the power system reduces the likelihood of the power system becoming unstable.

High-speed reclosing is another means of improving power system stability. Power transfer capability decreases for an out-of-service line. Automatic restoration of the line with minimal delay, allowing for only arc deionizing time, can also reduce the likelihood of the power system becoming unstable. If automatic restoration is used, both terminals must clear the fault instantaneously.

Clearing faults quickly reduces equipment damage and prevents unnecessary stress on the system, including through-fault damage to power transformers and insulator damage due to sustained arcing. Faster fault-clearing times also reduce the duration of the voltage sag from the short circuit and the resulting negative impact on power quality.

In a time-stepped distance application where there is a long line adjacent to a short line, it may not be possible to coordinate the reach of Zone 2 for the long line with the reach of Zone 1 for the short line. Pilot protection provides instantaneous fault clearing on the entire short line and facilitates coordination.

There are several types of pilot schemes used for high-speed protection, including the following:

- Permissive overreaching transfer trip (POTT).
- Directional comparison unblocking (DCUB).
- Directional comparison blocking (DCB).
- Direct transfer trip (DTT).
- Line current differential.

There are a few other variations of these schemes, but they are rarely used. This section examines the pros and cons of each scheme and discusses each of their teleprotection channel requirements.

A. Permissive Overreaching Transfer Trip

The POTT scheme, shown in Fig. 2, uses an overreaching Zone 2 element to trip the local breaker and send a permissive trip signal to the remote end. If the remote Zone 2 element detects a fault, the remote relay trips the breaker when it receives the permissive signal. Because the scheme uses an overreaching element to send permission, it needs additional supervisory logic to maintain security under current reversal conditions on parallel lines.

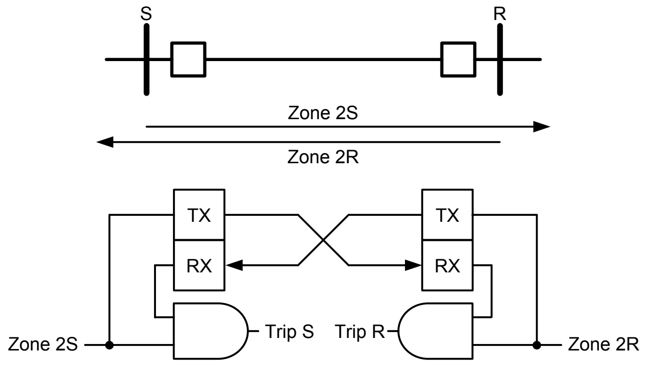

Fig. 2. POTT scheme simplified logic diagram

The relays are set to reach past the remote terminal (typically 120 to 150 percent of the protected line segment). The relay elements used to do this are typically distance (21) and/or directional overcurrent (67) elements, which means that the relays are set to detect faults in the forward direction. Forward distance and directional elements and a received permissive trip signal from the remote end allow tripping of the local breaker.

The POTT scheme is suitable for use with all digital teleprotection equipment applied over direct and multiplexed fiber-optic and radio systems. This scheme is inherently tolerant of propagation delays and channel asymmetry. POTT communications schemes need to provide high security and high speed (4 to 8 ms is typical).

B. Directional Comparison Unblocking

The DCUB scheme operates in the same manner as the POTT scheme with one variation. Additional logic is used to allow permission to trip for a brief period (typically 150 ms) during a communications failure due to noise on the channel. This additional signal is called unblock, as shown in Fig. 3.

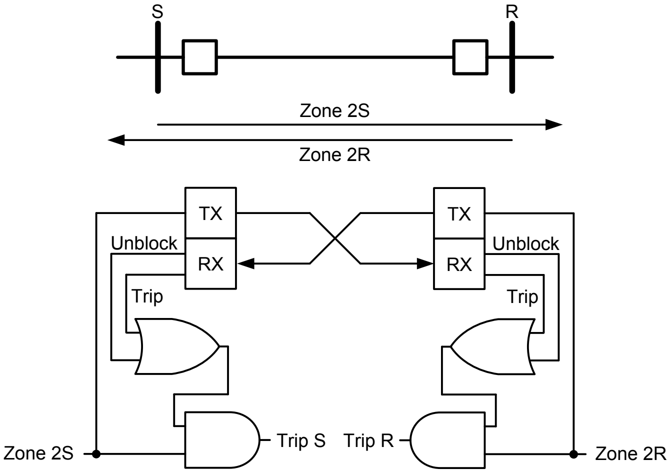

Fig. 3. DCUB scheme simplified logic diagram

The DCUB scheme is intended for use with frequency shift keying (FSK) PLC systems. The assumption is that the channel failure is due to the short circuit created by a fault on the protected transmission line. DCUB communications schemes need to provide high security and high speed (4 to 8 ms is typical).

C. Directional Comparison Blocking

Unlike the POTT and DCUB schemes, which send a trip signal when they detect a fault in the forward direction, the DCB scheme sends a blocking signal when it detects a fault in the reverse direction. The DCB scheme uses an instantaneous, reverse-looking element (referred to as Zone 3 in Fig. 4) to send the blocking signal. The Zone 3 element can be a nondirectional or directional overcurrent element or a reverse distance element. If the local Zone 3 element detects a reverse fault, it sends a blocking signal to the remote end, which prevents the line from tripping on an external fault. If the remote Zone 2 element detects a fault but does not detect a blocking signal, the remote relay trips the breaker after a short coordinating time delay (CTD). In many applications, a fast nondirectional element sends the blocking signal. In these cases, the blocking signal is quickly shut off if the fault is detected in the forward direction by the Zone 2 element.

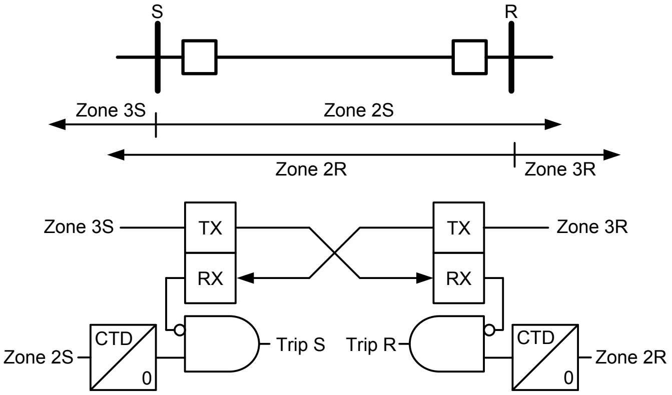

Fig. 4. DCB scheme simplified logic diagram

The DCB scheme is intended for use with on/off PLC systems. DCB communications schemes provide high-speed signaling (typically 1.5 to 5 ms). These schemes tend to be more dependable than secure because the DCB pilot channel is not required for tripping.

D. Direct Transfer Trip

The pilot schemes discussed up to this point have all been associated with line protection. The DTT scheme, as shown in Fig. 5, is used for equipment protection. The trip output of the receiver operates the lockout relay of a breaker. DTT is typically used for breaker failure schemes and is used to protect transformers that do not have breakers locally to interrupt power to the transformer when a transformer fault occurs.

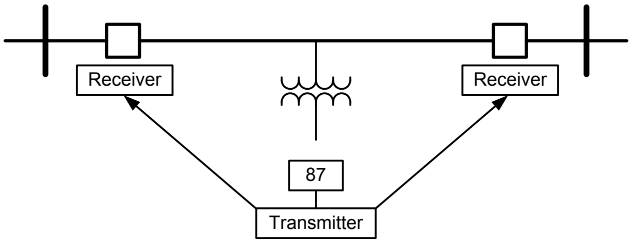

Fig. 5. DTT scheme for remote transformer protection

The DTT scheme is intended for use with FSK PLC and digital teleprotection systems. DTT schemes need to provide high security. This is usually accomplished using slower channel speeds (typically 8 to 12 ms), which are acceptable for this application.

E. Line Current Differential

From a communications perspective, line current differential protection is one of the most demanding line protection relay schemes to support.

The principle of differential protection is based on Kirchhoff’s current law, which states that all branch currents flowing into a node sum to zero. If the sum of the currents entering a protected element is not zero, there must be an unmeasured current and thus an internal fault. The current differential principle has the highest potential for security (it sees the external fault current entering and leaving the zone) as well as the highest potential for dependability (it sees the total fault current). When applied to power lines, the principle performs well on multiterminal lines, on very short and very long lines, and on series-compensated lines.

As discussed in [3], when used to protect transmission lines, line current differential protection requires long-haul communications channels to exchange current data as well as a synchronization method to align the currents measured at individual line terminals. Traditionally, the inherently distributed nature of line current differential schemes and the high cost of communications channels imposed limits on the amount of data that could be exchanged between line current differential relays, on channel latency, on the maximum number of terminals in the scheme, and on time synchronization. Historically, line current differential schemes have been implemented using fiber-optic cable directly connected to the relays or synchronous communications channels using multiplexed virtual channels within TDM-based systems.

The line current differential protection relay consists of multiple protection functions linked by a communications channel, as shown in Fig. 6 [4].

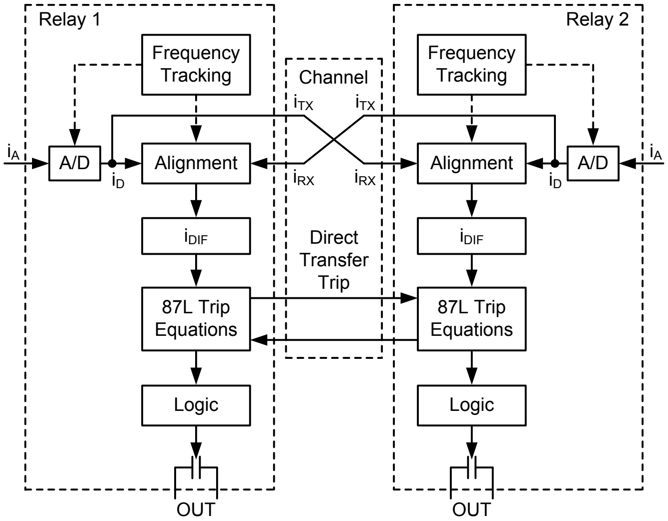

Fig. 6. Simplified architecture of a typical line current differential system

The following are the key channel performance requirements for line current differential applications:

- Availability is very high.
- Channel latency is 1 to 7 ms [1].
- Bit errors are 10^{-3} to 10^{-6}.
- Channel symmetry is less than 4 ms.

It is important to understand that channel latency is specified as a port-to-port propagation time that includes the buffering and processing of any active communications devices included in the line current differential channel. Similarly, asymmetry is specified as the difference between the transmit and receive port-to-port propagation times, including communications device buffering and processing.

IV. Power Line Carrier Systems

PLC was one of the first communications systems applied for pilot protection. The key advantages of PLC are that the power lines provide the media, there are no right-of-way issues, and the need to rely on third-party communications carriers is eliminated. Its disadvantages are that PLC systems require a higher level of maintenance than other communications technologies, and there is a chance that the fault noise produced on the protected line can interfere with the received signal. This interference is mitigated through boosting the output power for the command or trip state, which improves the system's SNR during fault conditions. Because of the unblock logic in the DCUB scheme, and the fact that the DCB relay scheme does not need to send the blocking signal through an internal line fault, the PLC protection schemes are very reliable.

PLC is ideal for providing pilot protection for long transmission lines that do not have an existing communications infrastructure.

There are two types of PLC modulation schemes: FSK and on/off modulation. On/off modulation is applied only with the DCB relay scheme. PLC operates in the 30 to 500 kHz frequency range. For an FSK scheme, the PLC transmitter output is typically 1 W in its quiescent state (guard) and 10 W in its command state (trip). For an on/off modulation scheme, there is no guard signal to monitor the health of the teleprotection channel, so automatic (checkback) testing is routinely performed. The PLC transmitter has a radio frequency output of 10 W for block. External 100 W power amplifiers can also be applied for longer protected line lengths.

PLC systems require special components to couple and decouple the carrier signals to the power line. Fig. 7 shows a simple one-line diagram of the components required to implement a PLC system. The PLC signal is coupled to the power line through a line tuning unit (LTU) and a coupling capacitor.

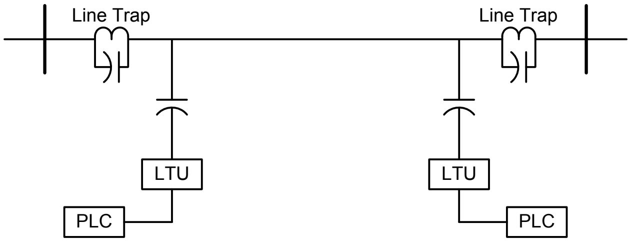

Fig. 7. PLC system components

The LTU is used to match the 50 Ω impedance of the carrier set to the line impedance. This allows the carrier signal to be coupled at its maximum power to the protected line and prevents signal reflections caused by impedance mismatches. The coupling capacitor, together with the series inductor in the LTU, provides a low-impedance path between the carrier set and the line at the carrier frequency range while providing a high impedance to the 60 Hz voltage of the power line. The line trap is an LC filter designed to contain the high-frequency signal of the carrier within the protected line segment while allowing the transmission line voltage and current to pass through.

PLC is still widely deployed and provides an effective solution for pilot protection.

V. Radio Systems

Radio systems provide an economical and reliable way to improve the security and dependability of power systems.

Most radio systems rely on a direct line-of-sight path between the transmitter and the receiver to establish a reliable communications link. As the distance between the transmitter and the receiver increases, the attenuation of the radio signal that carries the information also increases. The radio signal attenuation also depends on the carrier frequency (i.e., the frequency of the radio signal used to transmit and receive information). Radio system designers use the following simplified equation for the path loss (attenuation) between two radio antennas in free space:

$$L_P = 20\log\left(4d/\lambda\right) \quad (3)$$

where:

L_P is the path loss in decibels (dB).

d is the distance between the transmitter and the receiver.

λ is the wavelength of the radio frequency carrier in the same units as that of the distance.

Inspection of (3) shows that the path loss of a radio signal is directly proportional to the distance between the radios and the carrier frequency.

Radio systems provide flexibility and cost savings when compared with other communications methods such as copper and fiber-optic cables. Because the communications medium for radio systems is open, it is important to understand the probabilistic nature of the channel and its impact on applications that use radios. Other factors such as interference, jamming, eavesdropping, and spoofing should be considered when selecting this technology for teleprotection schemes [5].

The following equation is used by system designers to compute the link budget for a radio system:

$$P_R = P_T + G_T + G_R - L_P \quad (4)$$

where:

P_R is the received power in decibels-to-milliwatts (dBm).

P_T is the transmitted power in dBm.

G_T and G_R are the transmitter and receiver antenna gain in dB, respectively.

L_P is the path loss in dB.

This link budget can be represented using Fig. 8. The fade margin is the additional signal power received at the receiver above the required level that helps account for the interference from terrain, buildings, atmospheric conditions, and multipath fading that adversely affect radio propagation.

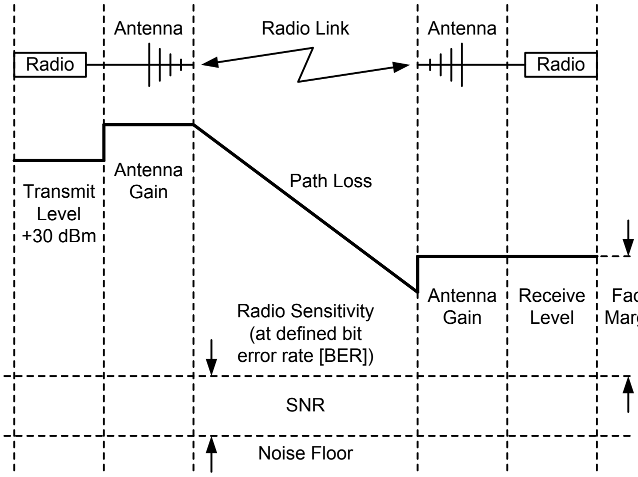

Fig. 8. Link budget for a point-to-point radio link

There are a variety of radio technologies available for applications in power systems. We categorized them as private and public networks in this paper.

A. Private Networks

Creating a private radio network involves setting up a standalone network with towers, antennas, surge arrestors, and radio equipment for communications between intelligent electronic devices (IEDs). These networks can be built using standard-based technologies or proprietary radio systems.

1) Standard-Based Radio Networks

These networks leverage existing standards to provide radio network connectivity. They also allow interoperability between devices from different manufacturers. Examples include Wi-Fi®, ZigBee® (which is based on IEEE 802.15.4), and Bluetooth®. In general, these standards were developed with specific applications in mind.

For example, Wi-Fi was developed for a radio local-area network operating indoors over a short range, and it can provide connectivity between a large number of devices. Wi-Fi operates in the 2.4 GHz or 5.8 GHz license-free band. The typical range for Wi-Fi in an outdoor environment is less than 1 mile. Wi-Fi networks are typically star-type networks, where the access point controls the traffic to and from and between the nodes communicating through the network. All of the devices on the Wi-Fi network are connected through the access point. Latencies through a Wi-Fi network depend on the network traffic and the loading of the access point and could have wide variations, from 5 to 50 ms or more. Wi-Fi is not recommended for high-speed protection due to its limited link range and propagation delay variances.

ZigBee and Bluetooth are radio packet access technologies with low data rates for short-range personal area networks. These operate with low bandwidth and high latency and are not recommended for protection applications.

2) Proprietary Radio Systems

These radio systems are networks built with specific application uses in mind. The customization of a radio protocol, hardware, or both provides capabilities that may not be achievable with standard-based networks. The systems can be designed in licensed frequency bands or in license-free frequency bands. Systems operating in a licensed band get a slice of the frequency spectrum exclusively for their own use. This can be advantageous for utilities because then they do not have to worry about other devices interfering with their radio networks. The transmit powers allowed in licensed bands are higher than the powers allowed in unlicensed bands, which enables long-range operation due to better radio link budgets. The downsides of these bands are that there can be several users competing to acquire small slices of the spectrum, the costs associated with acquisition can be high, and a slice of the spectrum simply may not be available.

There are proprietary radio systems designed to operate in the unlicensed spectrum, such as in the 902 to 928 MHz ISM band for North America or in the 2.4 to 2.46875 GHz band for worldwide operation. These license-free systems need to comply with regional regulatory requirements that dictate the maximum occupied channel bandwidth, transmit power, power spectral density, and so on. The benefit of using these bands is that no Federal Communications Commission (FCC) license is required. However, because these bands are popular and heavily used, they experience an increased level of noise and interference. There are technologies available today that mitigate interference by using techniques such as frequency hopping and direct-sequence spread spectrum. Radio systems operating in an unlicensed band are typically used in rural environments where interference from other radios is unlikely.

Proprietary radio systems can be built using the time-division multiple access (TDMA) or packet-based channel access methodologies. TDMA systems have a deterministic and repetitive transmission protocol assigned to specific users, data, or channels. The primary benefit of TDMA systems that makes them a good fit for teleprotection schemes is the low-jitter and low-latency communications that they offer. These systems are best suited for high-speed, low-latency command and control applications.

Packet-based systems are designed such that data are sent as a series of packets and multiple users have access to the same channel. Once a user gets access to the radio channel, the channel is locked for the entire period of the user's transmission. This provides some efficiency in usage of the radio channel, especially when multiple users are sharing the channel, but it comes at the expense of variability and high latency. Several standard-based systems that were previously described, such as Wi-Fi, are also packet-based systems. In wireline communications, Ethernet is the best example for packet-based systems.

Microwave radio links have long been used by electric utilities for the critical communications required for pilot protection schemes. Microwave radios are used for transferring control commands in pilot protection schemes between IEDs protecting the power lines. Microwave links use point-to-point technology and require direct line of sight for their operation. For critical infrastructure applications, network designers build systems using a combination of fiber-optic and microwave links to provide ring topologies when possible for better fault tolerance and communications reliability. Microwave radio systems typically transport TDM and/or Ethernet protocols. Typical microwave links operate in the licensed frequency bands between 6 to 40 GHz, but some manufacturers offer operation in both licensed and unlicensed bands for better flexibility. This flexibility comes from the ability to use existing 2.4 and 5.8 GHz antennas to build microwave radio links. Modern digital microwave radios with multicarrier modulation techniques can support radio link data rates of up to 300 Mbps or more. A typical microwave radio tower is shown in Fig. 9.

Fig. 9. Microwave dish antenna and tower

B. Public Networks

Machine-to-machine communications using cellular technology are growing with the increasing deployment of cellular phone networks in urban, suburban, and rural areas. The advantage of this technology is its built-in network infrastructure, which eliminates the need to set up separate antenna towers and potentially speeds up installation, enabling network connectivity to the end devices. Cellular networks operate in a variety of frequency bands, including 700, 800, and 900 MHz, depending on the carrier. Operation in these bands provides better penetration and propagation characteristics that can be advantageous in rural areas where the distance between an IED and the base station is long. For machine-to-machine communications, there is a vast variety of access technologies available, from 2G, 3G, and 4G, with cellular carrier companies claiming data rates of up to 100 Mbps.

Cellular networks are best suited for applications that require low data rates to the end devices.

When it comes to latency, the network latency for cellular systems is neither deterministic nor low. Typical latencies for devices communicating are in the order of 200 ms.

These networks are suitable for connecting devices that periodically report their status with small data sizes and for applications that can tolerate loss of communications. These networks are not suitable for teleprotection and high-speed restoration applications because of the nondeterministic nature of their latencies and their low service reliability [6].

For any radio system, it is important to consider the network design, site selection, path study, and equipment selection when deploying a robust radio solution. Network design includes all of the present and future traffic requirements, the network interfaces on the wired side, the protocols used for the application, and network system diagrams. Site selection and path studies include investigation of the topography for present and future conditions so as to compute the link budget for the radio system with adequate fade margins. For example, private networks with proprietary radio systems (like microwave, unlicensed, and licensed systems) require direct line of sight for their operation. In these cases, it is important to perform the site selection and path studies before deploying these systems.

C. Radio System Parameters for Power System Protection

There are some important radio system parameters that must be considered before applying them for protection applications. Unlicensed proprietary radio systems have the advantage of being lower cost compared with communications options like fiber. However, care must be taken to evaluate that the radio systems meet the same requirements as other available options. The following parameters must be evaluated for any radio system before applying it for protection and control.

1) Latency

Minimizing the latency of the radio link is critical for high-speed operations. When using radios for a pilot protection scheme or for high-speed control, the maximum allowed radio latency should be less than 10 ms. When evaluating radio latency, it is important to know the minimum and maximum latency for a good radio link. Very popular spread-spectrum radios always have a variable latency and, depending on radio design, will exhibit small or large variations in latency. The latency, along with the availability of the link, provides the real average, minimum, and maximum latency expected for a given operation.

2) Availability

Radio link availability is the ratio of the time the radio link provides good data to the total time the radio transmits data. Radio link availability varies based on the radio type and link parameters. Link availability is usually provided by the radio after it has been in operation. There are several ways to calculate radio link availability, but all yield close to the same results. Availability can be calculated using just the protocol data transferred or using the complete frame or radio link. Availability is given in a percentage and can go down to the detail of per-frequency availability. For either method, the link should be set up and run for at least a few days before using the availability numbers for long-term operation (for initially aiming the antennas, 10 to 20 minutes of operation is sufficient). Longer periods of successful in-service operating time yield higher availabilities. For protection and control applications, the widely accepted requirement for radio link availability is from 95 to 99.95 percent. This equates to between 265 and 438 minutes of outage per year. An availability of 95 percent is suitable for improving power quality or speeding up control with the primary operation already in place. An availability of 99.95 percent is sufficient for transmission lines requiring redundant protection systems. Availability and latency are used to calculate overall system performance.

3) Security and Dependability

Better link availability directly improves dependability. As described in Section II of this paper, better dependability indicates that when the system is called upon to operate, it operates within the latency required for the system in the presence of interference or noise. As availability decreases, dependability also decreases, so the system does not operate as needed.

Radio link security is highly dependent on the protocol used and the error detection capabilities of the radio.

VI. Fiber Optics

Fiber-optic-based communications are preferred for protection applications. Fiber transmission systems are immune to electrical interferences such as ground potential rise, electromagnetic interference (EMI), and radio frequency interference (RFI). For this paper, we categorize fiber-optic system applications into three types: direct connection, multiplexed using TDM, and multiplexed using Ethernet or packet technology.

A. Direct

Direct fiber is preferred by many protection engineers because no additional hardware is required and there is a single point of ownership. This method involves a direct fiber connection between two protective relays or teleprotection devices. For line current differential protection, the propagation delay is the speed of light through the fiber-optic cable (5 µs/km). The scheme reliability is high due to the direct fiber connection between the two relays. A direct fiber connection provides the lowest latency, highest reliability, and highest security.

The disadvantage of a direct fiber connection is that a pair of optical fibers (transmit and receive) needs to be dedicated for each set of pilot protection relays per line segment. Typically, there are not enough fibers available to deploy this method system-wide.

B. Multiplexed

A fiber-optic multiplexer increases the number of applications or circuits that can be carried over a single pair of optical fibers. Multiplexing substantially reduces the number of fiber pairs required to perform protection across the system. Multiplexers are not deployed as point-to-point devices, but they provide connectivity between many substations. Fiber use efficiency is further increased because multiplexers typically carry supervisory control and data acquisition (SCADA), engineering access, telephony, and security applications as well.

A multiplexer is an additional device inserted between the protective relay and the fiber. Additional hardware naturally reduces the reliability of the system. This is overcome through the multiplexer's design and supported topologies. Multiplexers designed for power system protection provide hardware redundancy to eliminate single points of failure. Multiplexer networks are typically deployed in a ring topology, which provides an alternate communications path should the primary fiber path be broken or damaged. These features combined provide increased reliability of the pilot protection relay schemes and the communications network.

1) *Time-Division Multiplexing*

As discussed in [7], TDM is a data communications method that interleaves multiple data streams over the same physical medium, giving each data stream a predefined, fixed-length time slot for using the physical channel. All data streams (subchannels) are allocated unique time slots on the physical channel.

Guaranteed bandwidth and data delivery times (determinism) are key advantages of TDM. The bandwidth in TDM networks is reserved for a configured subchannel, regardless of whether the channel is actually sending new information or not, which leads to a less efficient use of the physical medium compared with packet-based methods. TDM systems are therefore naturally suited to support applications that stream data steadily rather than send data in irregular bursts. Many TDM-based multiplexers designed specifically for power system protection applications have been available and deployed for many years. These multiplexers provide very low-latency performance when compared with their commercial telecommunications counterparts. Features such as fast ring healing times in the order of 5 ms or less, very low latency typically in the submillisecond range, and environmental hardening to allow for operation in uncontrolled environments at power system facilities are required for power system protection applications.

2) *Ethernet*

As discussed in [7], Ethernet is one of the most widely implemented packet-based technologies. Unlike TDM, Ethernet does not use the concept of preallocated time slots to send data. Instead, all applications share the same transport channel. Contention resolution methods deal with the challenge of having multiple packets arrive at the same time while trying to access the shared transport channel. In this situation, data packets build up rapidly in the buffer. If the system is heavily loaded with many applications trying to send large amounts of data, it is impossible to buffer all the data. Frames or packets are dropped if the network and bandwidth are not properly planned and designed. Higher-level protocols can deal with the detection of lost frames and can provide data retransmission. One method to ensure latency performance is to provide higher transport speeds. Ethernet transmission protocols like multiprotocol label switching (MPLS) and carrier Ethernet can provide fixed primary and backup circuit paths, which make Ethernet transport more deterministic. Restoration times for failed paths are approaching those of TDM-based synchronous optical network (SONET) systems (50 ms) but fall short of restoration times provided by protection multiplexers currently in use (5 ms).

The process of packetizing 64 kbps synchronous data used by line current differential relays and teleprotection systems adds additional latencies (7 to 10 ms) that bring overall pilot protection scheme delays back to those of the early pilot protection schemes.

Teleprotection and protective relay systems are slowly evolving toward Ethernet communications. SCADA and engineering access relay interfaces have made the transition already. This was relatively easy because Ethernet provides a simple solution for point-to-multipoint applications. Protective relays with Ethernet-based protection schemes are just starting to become commercially available. It will take some time for these devices to replace the TDM-based legacy devices currently in use. In the interim, commercially available telecommunications industry Ethernet multiplexers have not come close to matching the synchronous data circuit performance for legacy relay systems. Just as with TDM systems, the market will adapt and systems specifically designed for protection applications will become available.

As Ethernet-based teleprotection and line current differential communications schemes become more widely available, the latency issue will be solved. Ethernet transport systems are very efficient at transporting Ethernet data.

VII. Cybersecurity Practices

With the introduction of North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards, all communications, including teleprotection, must be evaluated for impact when the system falls under the bulk electric system definition. A good cybersecurity practice balances the four cybersecurity pillars to best meet the needs of the application. The four cybersecurity pillars are confidentiality, integrity, nonrepudiation, and availability.

Message confidentiality is used to protect the message contents from eavesdroppers. Message confidentiality is frequently required when usernames, passwords, or other sensitive data are sent as part of the message payload. Message confidentiality is achieved by the sending device applying a transform function to plain-text messages (human readable or binary) using secrets known only to the participating devices. The receiving device applies a reverse transform function on the encrypted messages to restore the messages back to their original plain-text form using the known secrets. Message confidentiality can be implemented on a communications-link basis or at the application layer. Link-level confidentiality transforms all messages using the communications link, but it requires every message to be transformed at each intermediary communications device. Communication at the application level is only transformed twice: once by the sender and once by the receiver. Confidentiality transformations also come in two types: block and streaming. Block transformations work on fixed-size messages (i.e., Advanced Encryption Standard [AES] works on fixed blocks of 128 bits). Streaming transformations work on much smaller data blocks, typically one plain-text digit at a time.

Message integrity is used to verify that the message has not been intentionally or unintentionally tampered with. Message integrity is typically implemented by the sending and receiving devices sharing a cryptographically sound hashing algorithm and secrets. The sending device hashes the message payload and appends the hash-based message authentication code (HMAC) to the message. Once the message is received, the receiving device recalculates the HMAC using the secret and verifies that the calculated HMAC matches the transmitted HMAC.

Nonrepudiation is very similar to message integrity, but it is used to verify the sender of the message instead of the contents of the message. Nonrepudiation requires asymmetric keys. Asymmetric keys (commonly called public/private keys) are not identical on the sending and receiving devices. Instead, the secret keys are paired to where the message transformation with one key can only be reversed with the other paired key. Because of this complex pairing relationship, transformations using asymmetric keys are very computationally expensive. Therefore, the nonrepudiation typically occurs in one of two ways. It can occur on a per-message basis, where the transformation is applied to the HMAC instead of the entire message payload. It can also occur on a per-session basis, where the receiver verifies the identity of the sender and then the pair dynamically generates a block session key known only to each device for message confidentiality and/or message integrity.

Availability provides the counterbalance to the other three cybersecurity pillars. Availability has two facets. First, the more transformations performed on the message, the less computational power and channel bandwidth is available for the primary purpose of the teleprotection scheme. Second, message confidentiality, message integrity, and sender nonrepudiation are all subject to noise on the communications channel. These methods cannot distinguish between intentional and unintentional tampering. Therefore, they treat all corruption as intentional tampering and discard the message.

The final and most important cybersecurity practice involving encryption is to verify that the encryption algorithms and implementations are cryptographically sound. Many encryption vulnerabilities are not on the algorithm itself but are instead in the implementation, such as the random number entropy. The National Institute of Standards and Technology Federal Information Processing Standard (NIST FIPS) validation process is one standard way to have confidence in both the cryptographic algorithm and in the implementation. Pilot protection schemes are point to point; therefore, signal spoofing and tampering have minimal effect on the bulk electric system.

VIII. Conclusion

There are many options available today to provide communications for pilot protection. Because of the availability of the communications media, several or all of these methods can be in use at a given power utility. The equipment and services available today have evolved using modern communications standards adapted to the performance requirements of high-speed pilot protection systems. This paper provides performance data for the systems that are intended to carry these specialized protection signals. A new challenge faced by protection engineers is the integration of the telecommunications and corporate information technology (IT) or communications departments. Much of the information and data provided in this paper has become tribal knowledge and is not fully understood by corporate IT communications departments. Today, high-speed fault clearing is more critical than ever because the power system has had to operate with lower margins. Faster fault clearing times allow operators to increase power flow on existing transmission corridors when the addition of new transmission lines is not possible. Power system stability is directly affected by the ability to clear or isolate faults at high speed.

IX. References

[1] ANSI C93.5-1997, American National Standard Requirements for Single Function Power-Line Carrier Transmitter/Receiver Equipment.

[2] IEC 60834-1:1999, Teleprotection Equipment of Power Systems – Performance and Testing – Part 1: Command Systems.

[3] B. Kasztenny, B. Le, K. Fodero, and V. Skendzic, “Line Current Differential Protection and the Age of Ethernet-Based Wide-Area Communications,” proceedings of the 45th CIGRE Session, Paris, France, August 2014.

[4] H. Miller, J. Burger, N. Fischer, and B. Kasztenny, “Modern Line Current Differential Protection Solutions,” proceedings of the 63rd Annual Conference for Protective Relay Engineers, College Station, TX, March 2010.

[5] S. V. Achanta, B. MacLeod, E. Sagen, and H. Loehner, “Apply Radios to Improve the Operation of Electrical Protection,” proceedings of the 37th Annual Western Protective Relay Conference, Spokane, WA, October 2010.

[6] S. T. Watt, H. Loehner, S. V. Achanta, A. Kivi, and B. Rowland, “Extending SCADA Networks Using Wireless Communications,” proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2015.

[7] K. Fodero and P. Robertson, “Combining TDM and Ethernet to Improve Network Performance for Mission-Critical Applications,” proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2015.

X. Biographies

Shankar V. Achanta received his M.S. in electrical engineering from Arizona State University in 2002. He joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2002 as a hardware engineer, developing electronics for communications devices, data acquisition circuits, and switch mode power supplies. Shankar currently holds three SEL patents, and he is an inventor on several patents that are pending in the field of precise timing and wireless communications. He currently holds the position of research and development manager for the precise time and wireless communications group at SEL.

Ryan Bradetich is a research and development manager for the wired networks product lines at Schweitzer Engineering Laboratories, Inc. (SEL). He received his BSCS in 1997, his MSCS in 2007, and his Ph.D. in 2012 from the University of Idaho. Ryan currently holds four patents and has several additional pending patent applications related to security and communications. Prior to joining SEL, he worked at Hewlett-Packard on the security team responsible for auditing and reporting the security status for approximately 20,000 UNIX and Windows® systems.

Ken Fodero is a business development manager for the communications product lines at Schweitzer Engineering Laboratories, Inc. (SEL). Before coming to SEL, he was a product manager at Pulsar Technologies for four years in Coral Springs, Florida. Prior to Pulsar Technologies, Ken worked at RFL Electronics for 15 years, and his last position there was director of product planning. He is a member of IEEE and has authored and presented several papers on power system protection communications topics.

Previously presented at the 2016 Texas A&M
Conference for Protective Relay Engineers.

20160205 • TP6717-01