Relay-to-Relay Digital Logic Communication for Line Protection, Monitoring, and Control

Kenneth C. Behrendt
Schweitzer Engineering Laboratories, Inc.

Revised edition released November 1998

Previously presented at the
12th Annual CEPSI Exhibition, November 1998,
International Conference Modern Trends in the Protection Schemes of Electric Power Apparatus and Systems, October 1998,
Beijing Electric Power International Conference on Transmission and Distribution, November 1997,
Power Delivery Asia '97/DistribuTECH Asia '97, September 1997,
51st Annual Georgia Tech Protective Relaying Conference, April 1997,
and 23rd Annual Western Protective Relay Conference, October 1996

Originally presented at the
32nd Annual Minnesota Power Systems Conference, October 1996

RELAY-TO-RELAY DIGITAL LOGIC COMMUNICATION FOR LINE PROTECTION, MONITORING, AND CONTROL

Kenneth C. Behrendt, P.E.
Schweitzer Engineering Laboratories, Inc.
Pullman, Washington USA

INTRODUCTION

Protection engineers, in concert with protective relay and communication product manufacturers, strive to achieve fast tripping for all transmission line faults through the use of communication-assisted protective relaying. Directional distance and overcurrent schemes, interfaced with communication equipment, send and receive logic-based information between relay terminals to determine if the fault is external or internal to the protected line section. Traditional relay schemes require costly external communication equipment. This paper discusses a new approach to achieve high-speed line protection, monitoring, and control using microprocessor-based relay-to-relay digital logic communication. Novel, cost-saving applications made possible by this new communication capability and considerations for communication channel selection are also presented.

RELAY LOGIC STATUS

Relay logic status is an integral part of protection, monitoring, and control schemes. When shared with other relays, relay logic status forms the basis for a relay scheme that improves upon the singular ability of a relay. Relay logic status includes the state of a relay element (picked up or dropped out), the state of an output contact (closed or open), and the state of a control input (asserted or deasserted). In terms of microprocessor-based relay logic, the status of a logic point is given a logical, or binary, value: 1 or 0. This digital relationship is the key to the new relay-to-relay logic communication discussed in this paper.

The most common example of shared relay logic status is the transmission line pilot "logic" [1] communication scheme. Relays operating independently at each line terminal must delay tripping for faults near the opposite line terminal to ensure coordination with relays at remote stations. Sharing relay logic status between schemes at each line terminal permits directional distance or overcurrent relays at both ends of a transmission line to trip with little or no intentional time delay for faults anywhere on the protected line section. This shared logic information forms the basis for permissive tripping schemes, intertripping schemes (direct or transfer tripping), and block tripping schemes.

[1] For the purposes of this paper, we differentiate between the pilot "data" communication scheme, such as a current differential scheme, which shares relay data between relays, and the pilot "logic" communication scheme, which shares relay logic status between relays.

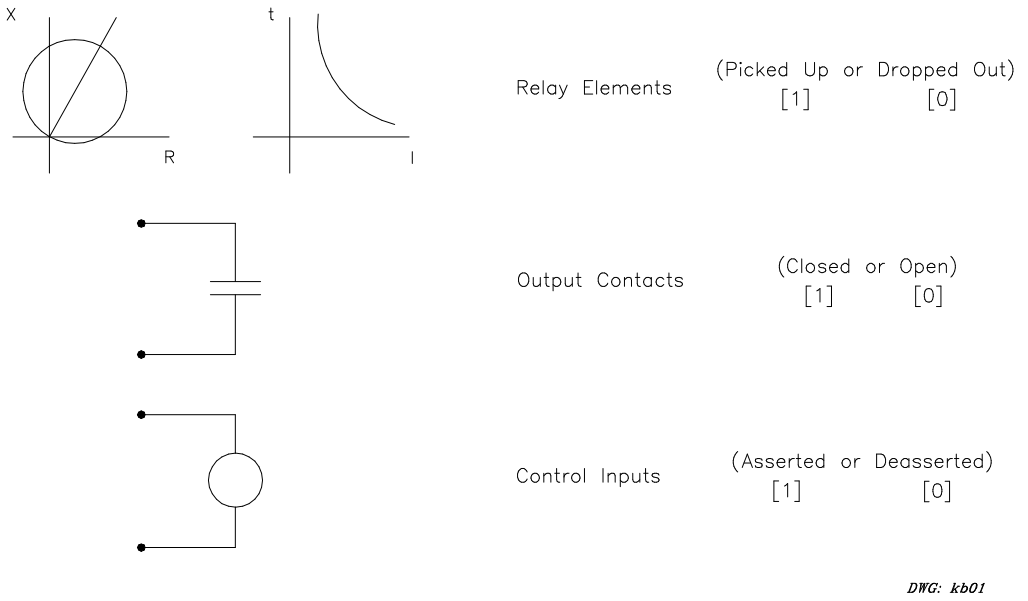


Figure 1: Relay Logic Status Elements

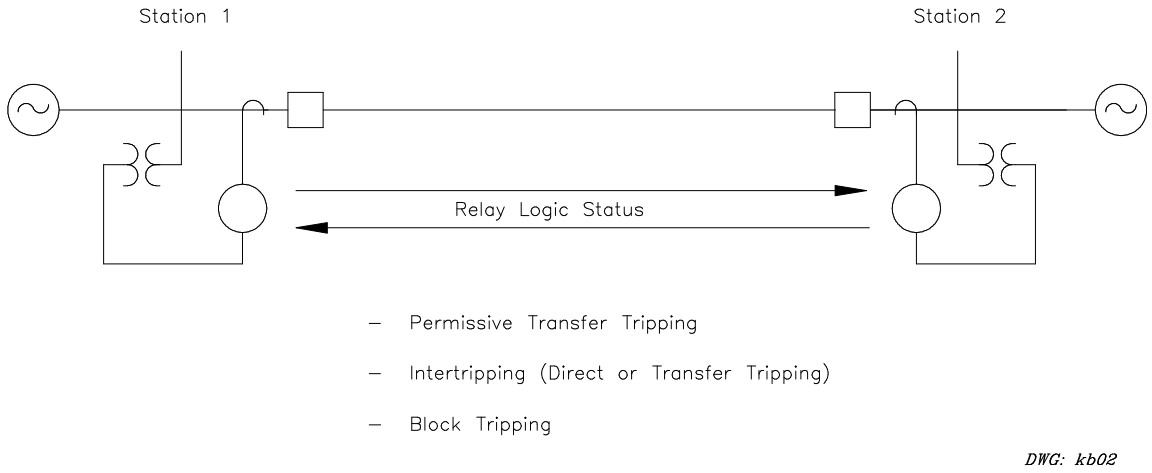


Figure 2: Relays Share Logic Status in Pilot Logic Communication Schemes

Other applications include remedial action schemes, status monitoring, and remote control—virtually any application that requires the communication of contact or logic point status to a remote location. Basic schemes may only need to share a single logic point, while more complex schemes may require sharing multiple logic points.

LINE PROTECTION PILOT SCHEME

Many types of line protection pilot schemes are in common use today, including Permissive Overreaching Transfer Trip (POTT), Permissive Underreaching Transfer Trip (PUTT), Directional Comparison Blocking (DCB), Directional Comparison Unblocking (DCUB), Direct Underreaching Transfer Trip (DUTT), and Direct Transfer Trip (DTT). Each of these schemes

requires the relay at one line terminal to communicate to the relay at the other line terminal that it either does or does not “see” a fault in the forward or reverse direction. Armed with this remote relay information, each relay quickly makes an informed decision to trip, if the fault is internal to the protected line section, or not to trip, if the fault is external to the protected line section.

Ideally, we might try to accomplish this communication by hardwiring a control circuit from an output contact on one relay to an input on the relay at the opposite line terminal.

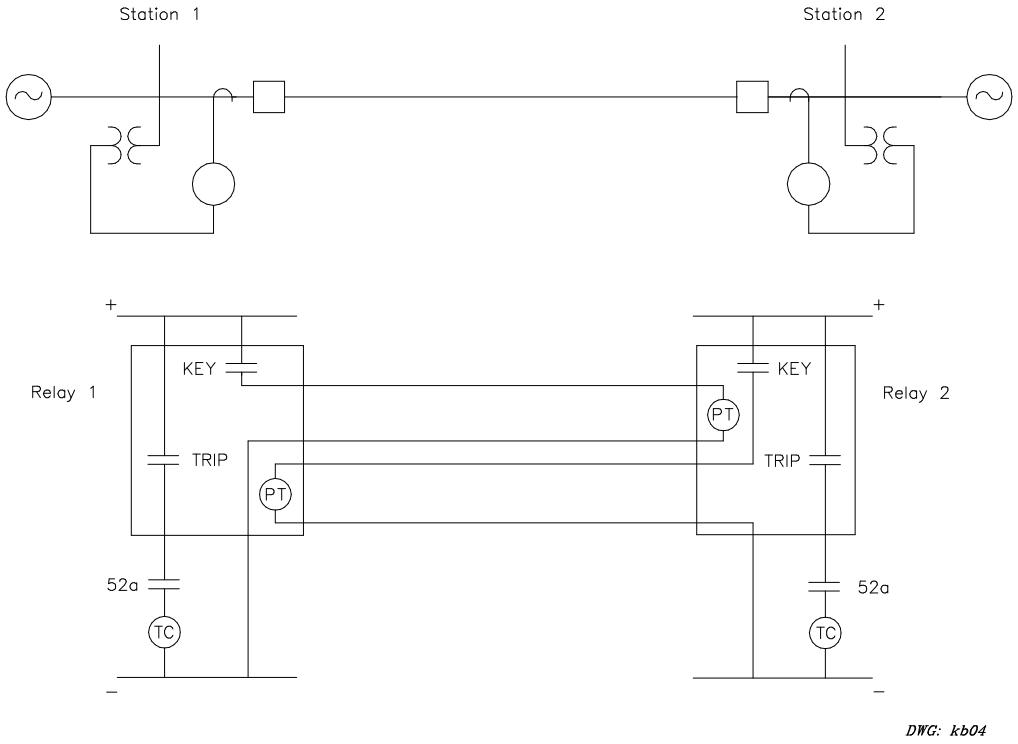


Figure 3: Ideal Permissive Tripping Pilot Communication Scheme With Hardwired Connections

If this direct connection were possible, it would provide simple, fast, secure, and reliable communication—all highly desirable attributes needed to achieve fast, secure, and reliable line protection. Adding logic communication channels would be as simple as wiring an additional contact at one relay terminal to a relay control input at the other relay terminal.

Unfortunately, the realities of physics prohibit us from making a simple, direct, hardwired metallic control circuit connection between relays. Ground potential differences, voltage drop, and induced voltages and currents present insurmountable obstacles to the direct metallic connection. As a result, a variety of alternate communication interfaces have been developed to achieve the desired result: relay logic status communication.

TRADITIONAL PILOT SCHEME LOGIC COMMUNICATION

Virtually all of the logic communication scheme techniques in service today were developed during the electromechanical and solid-state relay eras, some more than 40 years ago. The protective relays and communication equipment are separate and discrete devices that each serve a single purpose. The protection and communication devices are typically interfaced with an

electromechanical contact, although some solid-state relay systems may use transistor switches to electronically interface the devices. In any case, the device functions remain separate and distinct.

Most of these schemes convert a relay contact output to a safe and reliable communication signal that is transmitted from one line terminal to the other. At the receiving end, the signal is converted to a contact output, which is connected to assert a control input in the logic scheme of the relay.

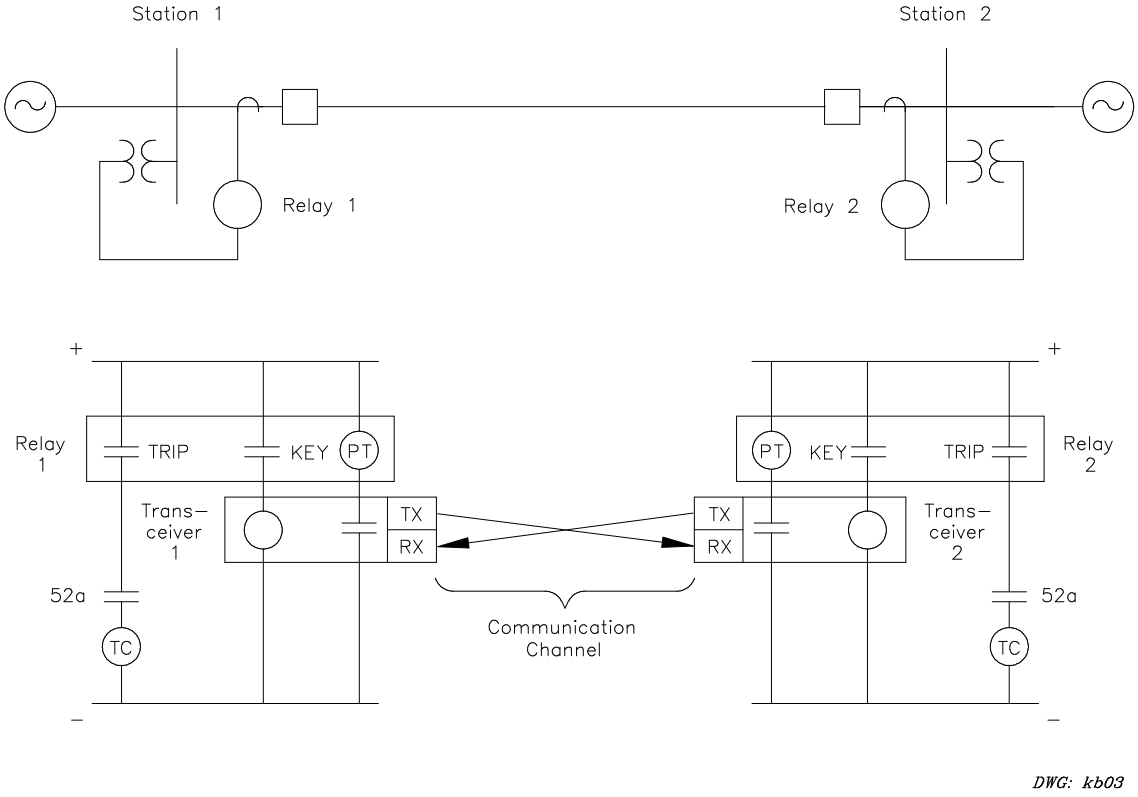


Figure 4: Traditional Permissive Tripping Pilot Communication Scheme With Separate Relay and Communication Equipment

Traditional pilot scheme communication equipment typically transmits and receives analog communication signals. Audio-tone signals (300 to 3,000 Hz) are most commonly used on leased or privately owned phone circuits, or on analog microwave radio. The low-frequency radio band (80 to 250 kHz) is commonly used for power line carrier communication. These techniques offer metallic isolation and signal filtering to provide safe and reliable relay-to-relay communication, but at a cost.

The communication equipment, which includes a combination of frequency generators, amplifiers, filters, isolating transformers, electronic logic, output relays, and control inputs, is expensive, sometimes exceeding the cost of the protective relays. Engineering, installation, panel space, wiring, setting, testing, and maintenance for separate communication equipment significantly adds to the basic equipment cost. These costs are compounded for each additional communication channel required.

Today, in the modern microprocessor-based relay age, these traditional communication techniques are still widely used:

- the communication equipment remains separate and distinct from the protective relay,
- the electromechanical contact remains the most common interface between the relay and communication equipment,
- and additional communication equipment and channel space are required for each additional relay logic status bit to be communicated.

All of these traits are carried over from the electromechanical relay era.

This contrast in technologies begs for a new, innovative approach to simplify and improve the process of sharing relay logic status between relay terminals.

A NEW APPROACH TO RELAY-TO-RELAY LOGIC COMMUNICATION

A new, innovative approach has been developed to share relay logic status between relays. This new approach takes advantage of the built-in communication capability and inherent digital logic processing capability of the microprocessor-based relay. Virtually every microprocessor-based relay has a communication port that is capable of sending and receiving digital messages. And the microprocessor-based relay processes digital data representing the status of relay measuring elements, control inputs, and control outputs. It's only natural that these two capabilities be combined to provide direct relay-to-relay digital logic communication.

The new, patented relay-to-relay logic communication technique repeatedly sends the status of eight programmable internal relay elements, encoded in a digital message, from one relay to the other through an EIA-232 serial communications port.

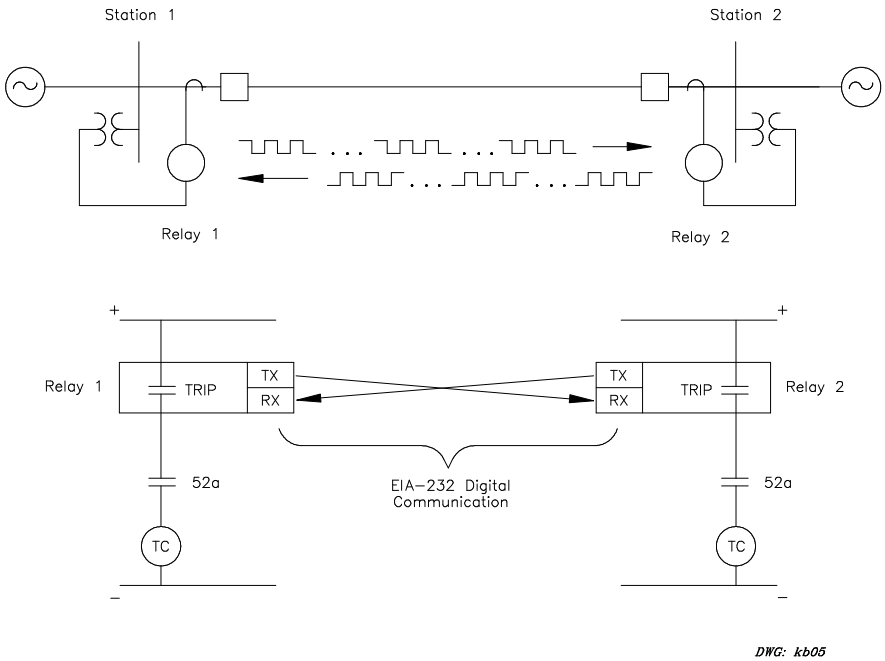


Figure 5: A New Approach: Direct Relay-to-Relay Digital Logic Communication

This new relay-to-relay logic communication technique creates eight additional "virtual" outputs on each relay, "wired" through the communication channel, to eight "virtual" control inputs on the other relay.

The eight "virtual" inputs, RMB1 to RMB8, are internal relay elements in the receiving relay that follow, or "mirror", the respective status of the TMB1 to TMB8 "virtual" outputs in the sending relay, as shown in Figure 6.

The logical status of each Receive *Mirrored Bit*, RMB1 through RMB8, in one relay "mirrors" the logical status of each respective Transmit *Mirrored Bit*, TMB1 through TMB8, in the other relay. A change in the TMB1 status of Relay 2 from a logical 0 to a logical 1 causes the RMB1 status of Relay 1 to change from logical 0 to 1. This creates a virtual connection between the two relays as the Receive *Mirrored Bits*, RMBs, of one relay follow the status of the respective Transmit *Mirrored Bits*, TMBs, sent from the other relay.

Each Transmit *Mirrored Bit* is programmed, just as you would an output contact, with a logic equation that represents the status of an internal relay element, control input, output contact, or any combination of these. Each Receive *Mirrored Bit* is assigned a function, just as you would assign a function to a control input. These assignments include functions such as permissive trip, block trip, 52A status, etc.

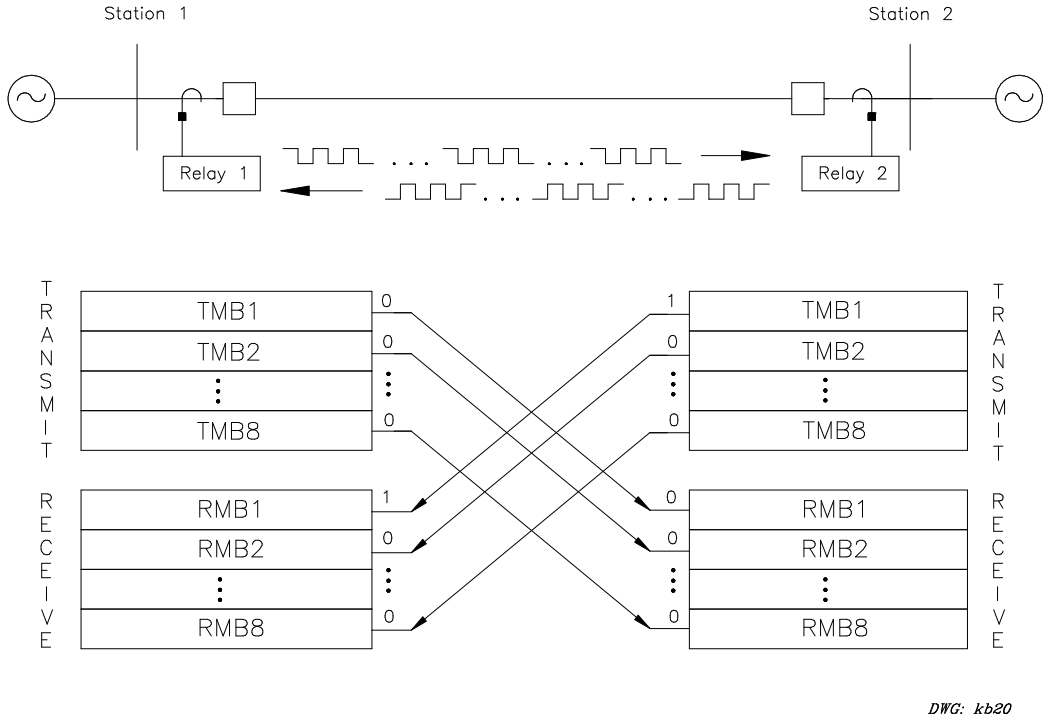


Figure 6: Relay-to-Relay Logic Communication

This new approach produces the equivalent of eight traditional relay communication channels between relay terminals, significantly increasing the functionality and cost effectiveness of the communication media. This new approach also eliminates the need for the expensive traditional communication equipment, which is replaced by much more cost-effective channel interface devices. The considerations for choice of communication media, and the corresponding channel interface devices, are discussed later in this paper.

Communication channel security and dependability are important aspects in traditional communication schemes, and they are equally important with the new relay-to-relay logic communication scheme. In traditional schemes, the communication equipment performs the necessary signal integrity checks before handing the message to the relay system. In the new relay-to-relay logic communication scheme, the relay assumes the responsibility for digital message security.

Digital Message Security

Each relay-to-relay logic communication digital message sent from one relay to the other consists of two bytes, where each byte contains eight data bits. Each byte of the message carries part of the eight relay logic status bits representing the programmable Transmit *Mirrored Bits* logical status. Figure 7 shows the relative position of the status of each bit in each message frame. The status of each bit is represented as a logical 0 or 1 in the digital message.

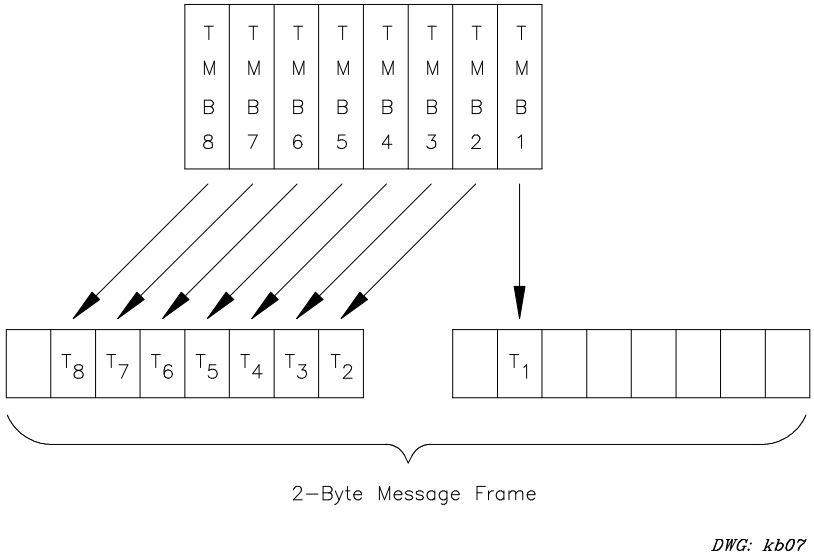


Figure 7: Relay Logic Status Bits in Digital Message Frame

Multiple security measures are used to ensure that the eight relay logic status elements are correctly communicated from one relay to the other. Each byte of the 2-byte message has a 1-bit byte flag to identify the correct byte sequence. The second byte of the message includes a 6-bit Cyclic Redundancy Check (CRC) table calculated from the status of the eight relay logic status bits.

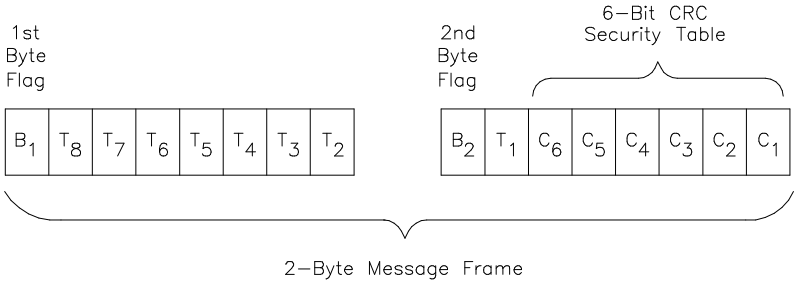


Figure 8: Byte Flag and CRC Security Bits in Message Frame

Each byte of the asynchronous message is preceded by a start bit and followed by up to three bits, which can include one or two stop bits and a parity bit as shown in Figure 9.

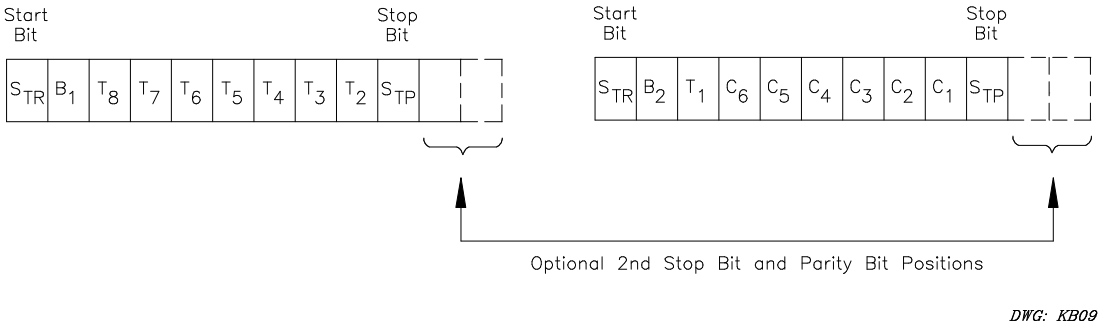


Figure 9: Asynchronous Message Framing Bits

The relay checks each message to ensure the byte flags are in the correct order; calculates a CRC value from the received message bits and checks that it matches the received CRC; checks message framing for proper start, stop, and parity bits; and performs a timing test to ensure that a message is received for each message sent. If any of the checks fail, the erroneous message is rejected. For added security, several good messages must be received before the relay again begins accepting messages and processing the logic status bits.

Security and Dependability Controls

Because message integrity is checked in the relay, appropriate control can be applied to accept, reject, and time-delay received logic status changes. This permits you to determine the level of security and dependability needed for your particular application. For instance, direct tripping applications may dictate a higher security level than permissive tripping applications. You can add security to an application in two ways:

- Introduce a short pickup time delay on the output of the received logic status bit. This short pickup time delay requires more than one direct trip message to sustain the trip output initiate. And, as shown in Figure 10, supervise the trip output with the relay message security bit to ensure that no output occurs unless the relay continues to receive good messages.

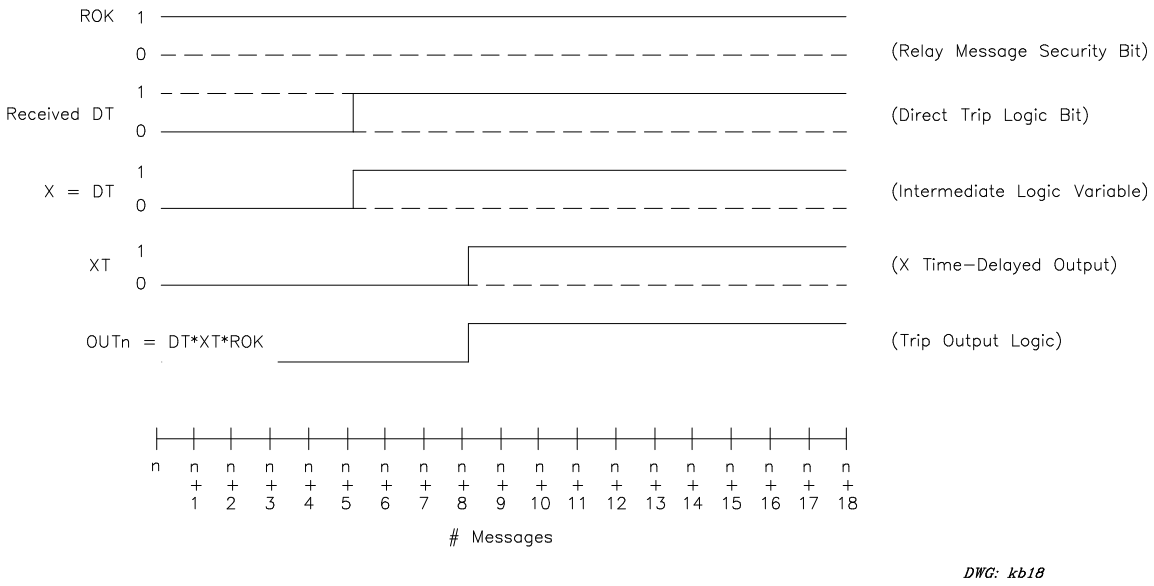


Figure 10: Relay Logic Technique for High-Security Pilot Scheme Applications

- Set two or more transmit logic status bits with the same initiate, and set the corresponding receive logic status bits with different outputs. Then AND(*) the received logic status bits together to form the output as shown in the table below:

Relay 1	Relay 2
TMB1 = 3PT	RMB1 = DT
TMB2 = 3PT	RMB2 = LP1
	OUT1 = DT * LP1

Dependability is enhanced by permitting action even if occasional bad messages are received, as is typically done with permissive tripping schemes where you expect that a line fault may adversely affect the communication channel. You can permit tripping if bad messages occur coincidentally with fault detection using the relay logic shown in Figure 11. With this logic, the output of the receiving relay is permitted to operate if either overreaching Zone 2 distance element, phase (M2P) or ground (Z2G), picks up at the same time the communication channel goes down. A timer output (YT) is used to limit the duration of the permitted trip.

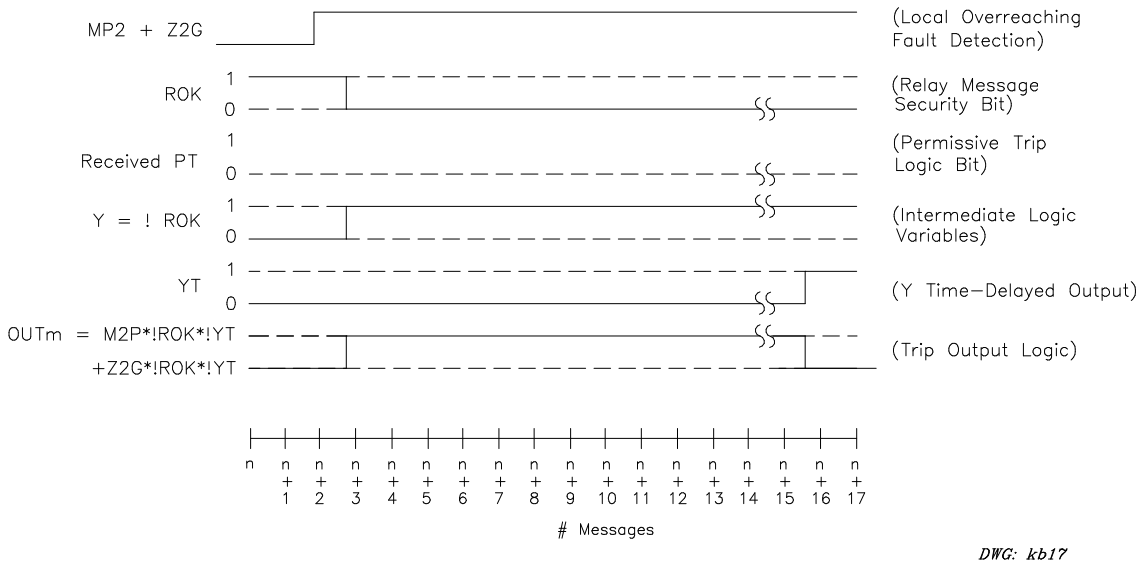


Figure 11: Relay Logic Technique for Dependable Pilot Scheme Applications

Relay-to-Relay Logic Communication Performance

Performance of the new relay-to-relay logic communication technique compares favorably with traditional communication schemes, although some parameters may not be directly comparable. Speed, which is a measure of the time it takes to assert an element in the receiving relay after an initiating logic status change in the transmitting relay, may be the most comparable aspect. In general terms, the nominal back-to-back operating time is 6.3 milliseconds at 9,600 or 19,200 bits per second communication rate. This back-to-back operating time does not include the channel interface and propagation delays, which will be affected by the choice of communication channel, as will be discussed later in this paper.

In comparison, typical audio-tone equipment has a back-to-back operating time of 8 to 12 ms, depending on bandwidth. This does not include the operating time of the initiating relay output contacts and the processing time of the control input on the receiving relay, which can add several milliseconds. The channel propagation delay will also adversely affect the overall operating speed.

	Traditional Analog Communication	Relay-to-Relay Digital Communication
Relay Output Contact Time	3.5 ms	None
Back-to-Back Operate Time	8 - 12 ms[1]	4.2 - 6.3 ms[2]
Relay Control Input Processing Time	2.1 ms	2.1 ms
	13.6 - 17.6 ms	6.3 - 8.4 ms

1) 8 ms for wide band, 12 ms for narrow band
2) 9,600 baud

Figure 12: Speed Comparison: Traditional vs. New Relay-to-Relay Logic Communication

Security and dependability of the new relay-to-relay logic communication technique are much more difficult to relate to the traditional communication schemes. Traditional schemes using analog communication signals measure channel performance in terms of signal-to-noise ratio (SNR). Analog transmitter output power and receiver input sensitivity are measured in decibels (db). The receiver must distinguish between good signal and unwanted noise. The ability to make this distinction depends heavily on the design of the receiver, which is beyond the scope of this paper. For the most part, the security and dependability of traditional analog communication schemes is not an issue.

In digital communication, the channel performance is measured in Bit Error Rate (BER), expressed in number of bit errors per number of bits transmitted. A bit error is a flipped bit, where a bit transmitted as a logical "1" is received as a logical "0," or vice versa. It is not uncommon for digital communication channels to have a 10^{-9} BER, which means that, on average, there is 1-bit error or one flipped bit per one billion transmitted bits.

As discussed earlier, the new relay-to-relay logic communication scheme applies multiple message security checks, including a 6-bit Cyclic Redundancy Check (CRC), to check for bit errors. The general polynomial for a 6-bit CRC is:

$$g(x) = x^6 + x^5 + x + 1 \qquad \text{Equation 1}$$

The 6-bit CRC will detect all possible combinations of one, two, or three flipped bits in the same message. Some combinations of four or more flipped bits in the same message may go undetected. For this reason, it is important to understand the probability of these undetected errors. The probability of a bad message getting through undetected can be analyzed using statistical probability techniques. Probability analysis for channel security and dependability is included in Appendices A and B. The results clearly show that the relay-to-relay logic communication channel security is very nearly unity (1.0) over a wide range of Bit Error Rates. Likewise, communication channel dependability approaches unity for Bit Error Rates less than 10^{-4}, which is a relatively high BER, indicative of a poor communication channel.

ENHANCED PILOT SCHEME APPLICATIONS WITH RELAY-TO-RELAY LOGIC COMMUNICATION

Traditional pilot scheme applications transmit one logic status bit between relay terminals. The new relay-to-relay logic communication technique, with the ability to transfer up to eight logic status bits in one message, greatly expands the capability of the pilot scheme to perform other functions. For comparison purposes, we examine a typical permissive overreaching transfer tripping scheme to see how easily this scheme is enhanced to accomplish other functions.

Basic Permissive Overreaching Transfer Tripping Scheme

In the basic permissive overreaching transfer tripping pilot communication scheme, the Zone 2 overreaching relay element keys permissive tripping logic to the remote relay terminal, permitting the remote relay to trip its breaker if it sees a fault in the forward direction. The scheme also keys permissive tripping logic if the local breaker is open (!52AA1 = NOT 52A).

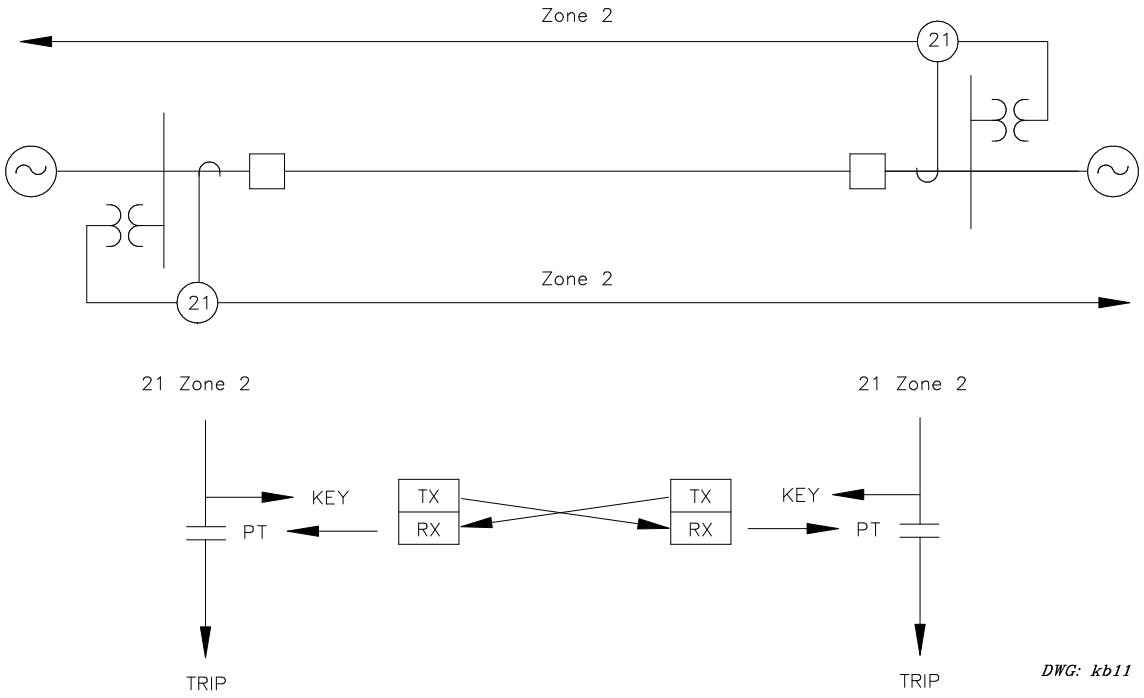


Figure 13: Basic Permissive Overreaching Transfer Tripping Pilot Communication Scheme

This basic logic is implemented with relay-to-relay logic communication using the transmit and receive logic status assignments shown in Table 1. All other relay-to-relay logic status elements, TMB2 to TMB8 and RMB2 to RMB8, are not assigned (na).

Table 1: Basic Permissive Overreaching Transfer Trip Relay-to-Relay Logic Communication Settings

Relay 1	Relay 2
Transmit Logic	**Transmit Logic**
7TMB1 = **KEY + !52AA1**	TMB1 = **KEY + !52AA1**
TMB2 … 8 = na	TMB2 … 8 = na
Receive Logic	**Receive Logic**
RMB1 = **PT**	RMB1 = **PT**
RMB2 … 8 = na	RMB2 … 8 = na
Partial Output Logic	**Partial Output Logic**
OUT1 = **3PT**	OUT1 = **3PT**

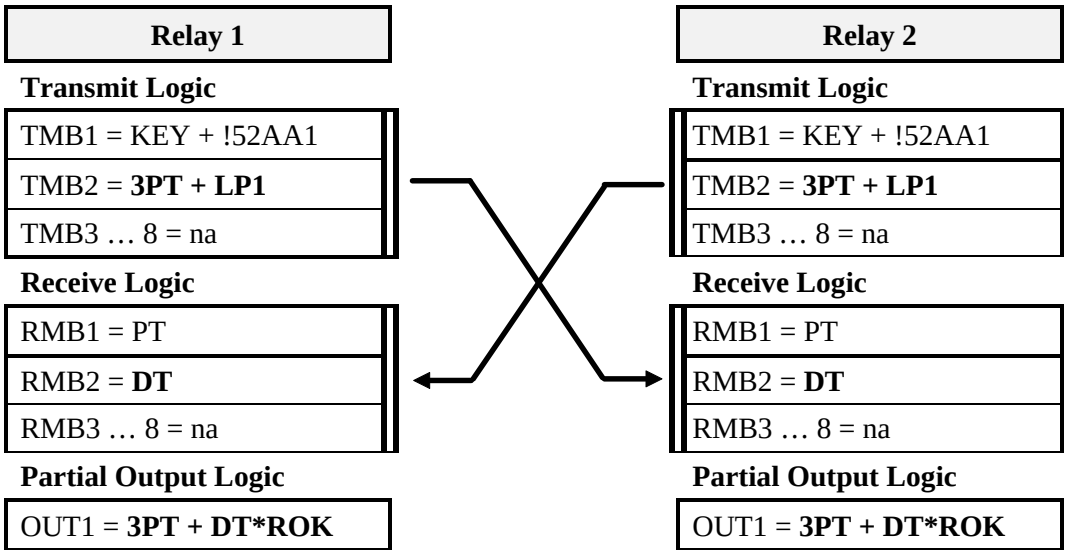
Setting TMB1 bit to KEY is equivalent to connecting a Zone 2 overreaching relay output contact to the keying input on a communication device. Likewise, assigning RMB1 to PT is equivalent to connecting the communication device output contact to a permissive trip input in the relay scheme. In this example, relay output contact OUT1 is connected to trip the local breaker when relay three-pole trip logic (3PT) asserts.

POTT Plus Direct Transfer Tripping

The basic POTT scheme logic is easily enhanced using relay-to-relay logic communication. For instance, to ensure that the remote line terminal breaker trips when the local relay trips the local breaker, you can establish a direct transfer tripping channel using another transmit and receive logic communication bit. To accomplish this, simply set TMB2 = 3PT to assert TMB2 when the local relay three-pole trip logic asserts, and set the associated RMB2 = DT to assert the direct trip logic when the RMB2 bit asserts. Then program the breaker tripping output contact to operate for any 3PT OR (+) DT element assertion. You can add a level of security to the direct transfer trip output by ANDing DT with the relay-to-relay logic communication status element, ROK. As long as the messages continue to pass all security checks, ROK remains asserted. When a bad message is detected, that message is rejected, and ROK deasserts.

Likewise, add direct transfer tripping functions for transformer, bus, or breaker failure relay operations simply by ORing their respective relay inputs (LP1 shown in this example) with the 3PT element in the TMB2 setting.

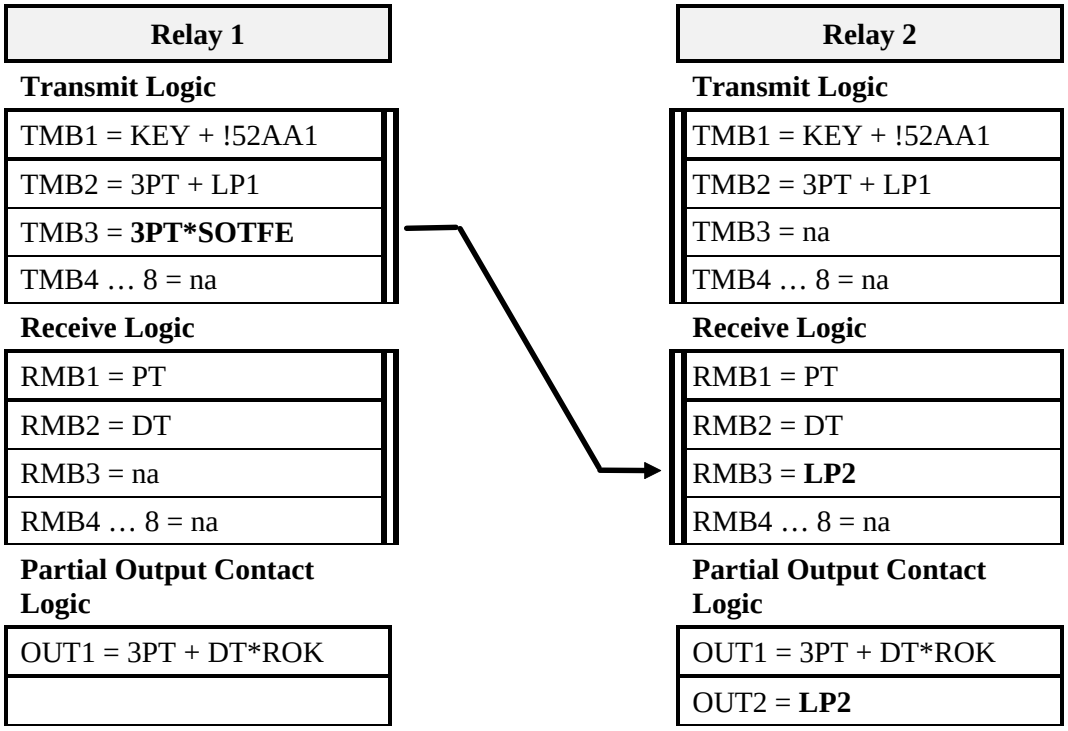
Table 2: POTT Plus Direct Transfer Tripping Pilot Scheme Logic



POTT Plus DT Plus Remote Reclose Blocking

Another pilot scheme enhancement that is easy to accomplish with relay-to-relay logic communication is remote reclose blocking. After tripping both line terminals for a fault, automatic reclosing is used to close both line breakers. By staggering the reclose times, you can use relay-to-relay logic to remotely block the second terminal reclose operation if the first terminal closes into a fault. This logic uses the relay's switch-onto-fault logic element, SOTFE, in combination with the three-pole trip element, 3PT, to assert one of the relay transmit logic bits (TMB3 in this example). This, in turn, asserts the associated receive logic bit, RMB3, in the remote relay, which is assigned to a programmable input element, LP2. The programmable input element, LP2, is then used to block reclosing—internally if reclosing logic is programmed in the relay or externally, through an output contact, if a separate reclosing relay is used.

Table 3: POTT Plus DT Plus Reclose Blocking (RB) Pilot Scheme Logic

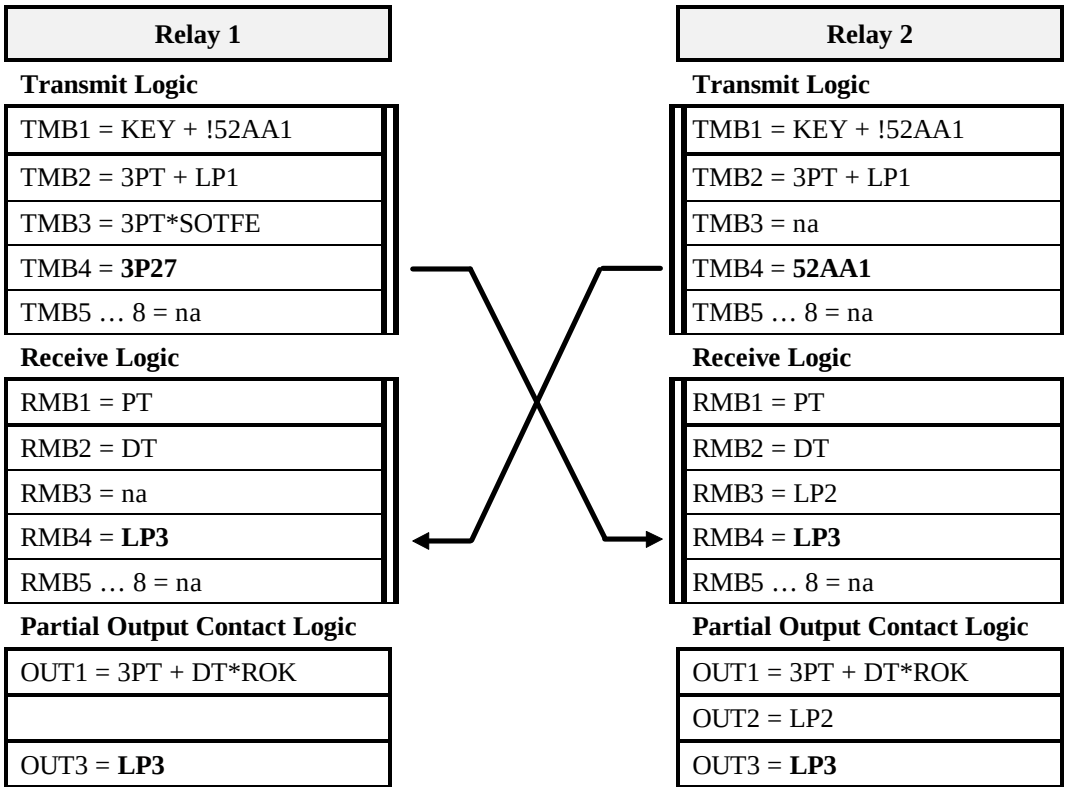


Remote Monitoring

It is often desirable to remotely monitor the status of a device, such as a line breaker, or a condition, such as bus undervoltage, at the remote line terminal. This has applications for protection, control, or monitoring and is easily accomplished with relay-to-relay logic communication. Simply program the transmit logic bit with the appropriate relay element, either internal or external, and assign the corresponding receive logic at the remote relay with a logic input. Use the assigned logic input in an internal control equation, or set an output contact to follow the remote input, as shown in this example.

In this example, we use Relay 1 to remotely monitor the breaker 52a status at the Relay 2 line terminal and, in the other direction, we use Relay 2 to remotely monitor the voltage status of the bus at the Relay 1 line terminal. The 52a breaker status is represented by a breaker 52a contact control input represented by an internal relay element, 52AA1, in Relay 2, and the bus voltage status is represented by a three phase undervoltage element, 3P27, in Relay 1.

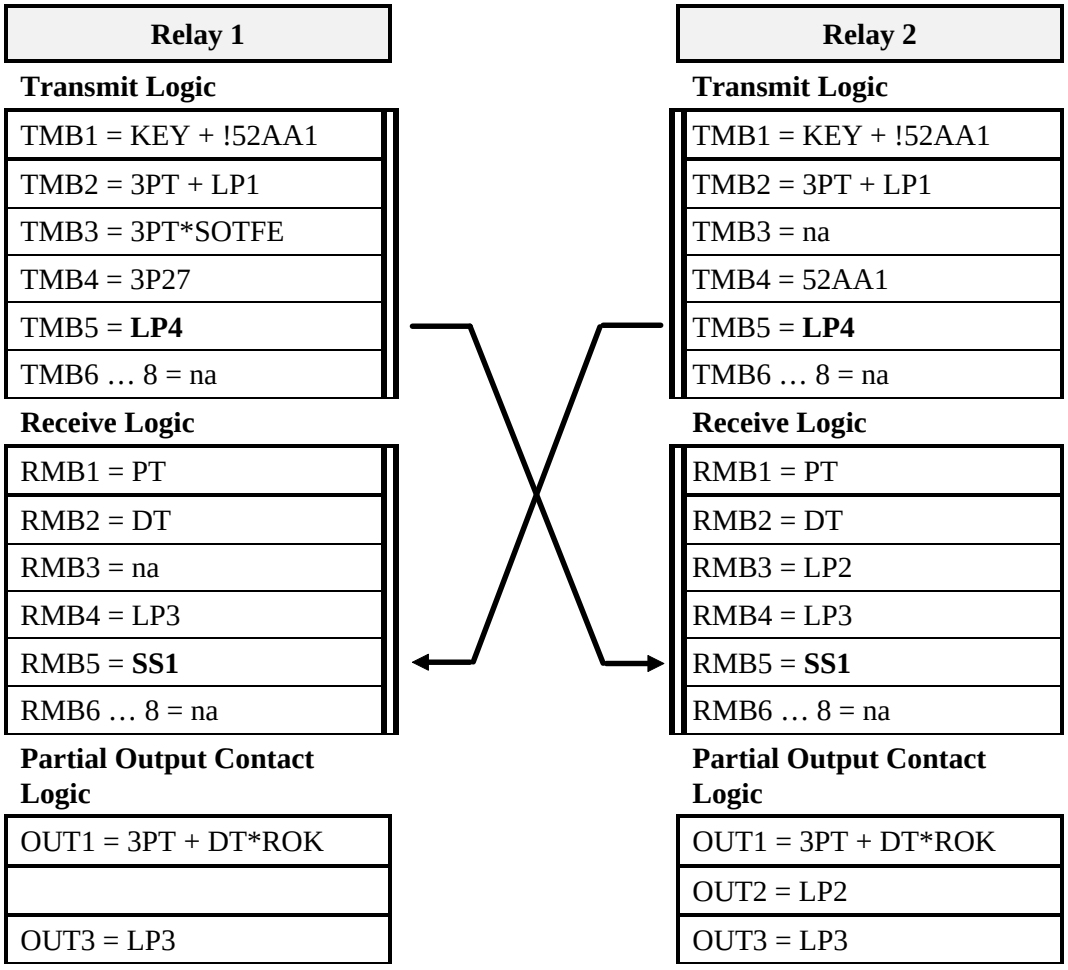
Table 4: POTT Plus DT Plus RB Plus Remote Monitoring (RM)



Remote Setting Change

Connect a control switch contact, or a SCADA RTU control contact, to a relay control input at one line terminal, and program the input to change relay settings on the local and remote relays at the same time. Likewise, use an internal relay element, or a substation device contact, to automatically change local and remote relay settings to create an adaptive relay scheme. Table 5 shows an example where TMB5 is set to follow a programmable bit, LP4, which is assigned to monitor a relay control input. When LP4 asserts, the local TMB5 logic element asserts the remote RMB5 logic element, which is programmed as a setting selector switch input, SS1. When this element asserts, the relay changes group settings based on a predetermined selector switch position table.

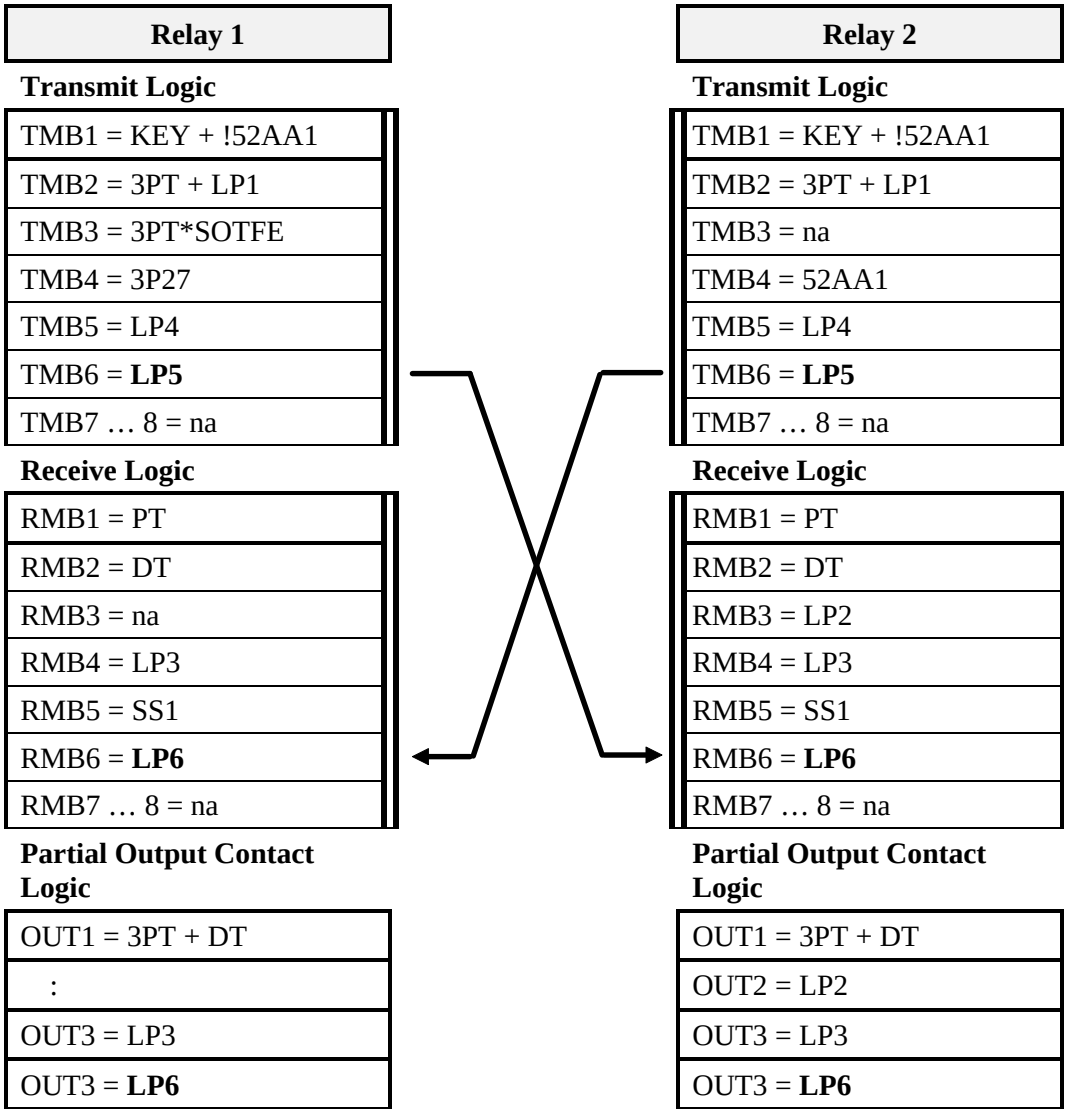
Table 5: POTT Plus DT Plus RB Plus RM Plus Remote Setting Change (RSC)



Remote Control

Just as we used the new relay-to-relay logic to remotely change relay settings in the previous example, the same technique is used to remotely control a device at the opposite line terminal and substation. A control switch contact, SCADA RTU control contact, or device control contact is connected to a relay control input, assigned as LP5 in this example, which is programmed to assert a transmit logic status bit, TMB6. TMB6, in turn, drives the remote receive logic status input, RMB6. Logic status input RMB6 is assigned to assert programmable input element LP6, which, in turn, is programmed to operate output contact OUT3 when remote control input is asserted. The relay output contact is connected to control a substation device, such as a breaker.

Table 6: POTT Plus DT Plus RB Plus RM Plus RSC Plus Remote Control (RC)



Relay 1
Transmit Logic
TMB1 = KEY + !52AA1
TMB2 = 3PT + LP1
TMB3 = 3PT*SOTFE
TMB4 = 3P27
TMB5 = LP4
TMB6 = **LP5**
TMB7 … 8 = na
Receive Logic
RMB1 = PT
RMB2 = DT
RMB3 = na
RMB4 = LP3
RMB5 = SS1
RMB6 = **LP6**
RMB7 … 8 = na
Partial Output Contact Logic
OUT1 = 3PT + DT
:
OUT3 = LP3
OUT3 = **LP6**

Relay 2
Transmit Logic
TMB1 = KEY + !52AA1
TMB2 = 3PT + LP1
TMB3 = na
TMB4 = 52AA1
TMB5 = LP4
TMB6 = **LP5**
TMB7 … 8 = na
Receive Logic
RMB1 = PT
RMB2 = DT
RMB3 = LP2
RMB4 = LP3
RMB5 = SS1
RMB6 = **LP6**
RMB7 … 8 = na
Partial Output Contact Logic
OUT1 = 3PT + DT
OUT2 = LP2
OUT3 = LP3
OUT3 = **LP6**

Summary

To summarize our example, we have accomplished several typical pilot communication scheme functions with one communication channel connected directly between relays at each line terminal as shown in Figure 14, below. In fact, we have spare relay-to-relay logic status elements available for other functions, or these spare elements can be used to add security to direct tripping functions, as discussed earlier.

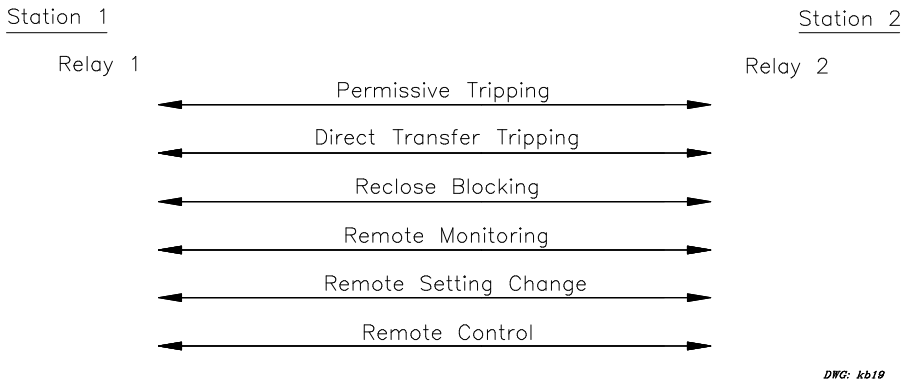


Figure 14: Summary of Relay-to-Relay Logic Communication Example

RELAY-TO-RELAY LOGIC COMMUNICATION CHANNEL CONSIDERATIONS

Direct Digital Communication via Fiber-Optic Cable

Direct digital relay-to-relay logic communication via direct fiber overcomes the problems of ground potential rise and interference problems encountered with metallic cable. A fiber-optic transceiver is used at each relay terminal to convert the relay's EIA-232 signal to an optical signal that can be transmitted over fiber-optic cable. Present multimode fiber-optic cable and transceiver technology supports optical signal transmission up to two or three miles (three to five kilometers). Longer distance transmission, from several miles, up to over 50 miles, is achieved using single mode optical cable and transceivers. Current cost of the fiber optic transceivers ranges from a few hundred dollars for each multimode transceiver to around one thousand dollars or more for each single mode transceiver.

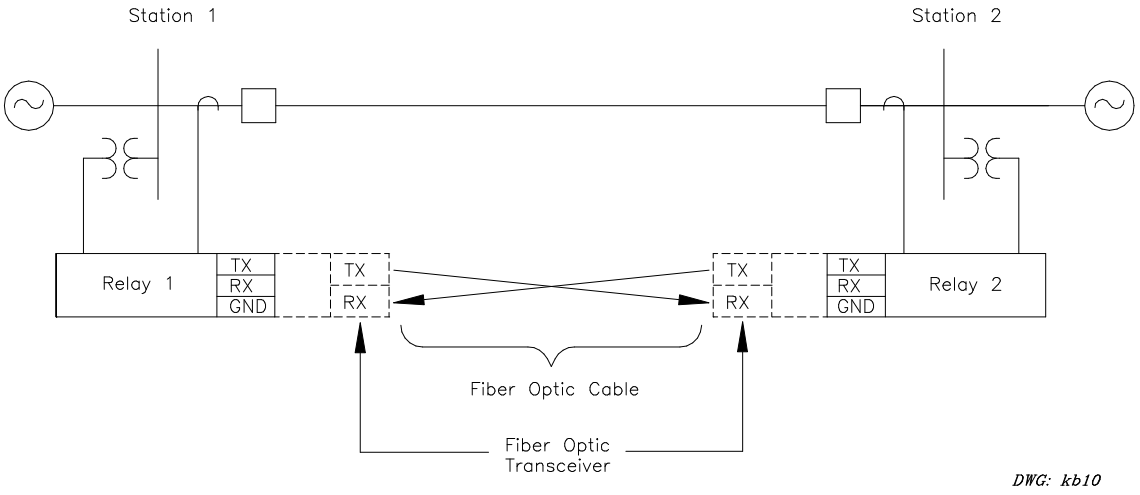


Figure 15: Direct Digital Communication via Direct Fiber-Optic Cable

Direct fiber-optic cable communication is the simplest, most straightforward media for relay-to-relay logic communication. It is virtually immune from electrical interference and typically has a bit error rate below 10^{-9}. Data delay in the fiber-optic transceivers and optical cable is typically

measured in the tens of microseconds or less, which is negligible compared with the data transfer rate between relays.

Digital Communication via Network Communication Multiplexers

Communication multiplexers interface individual communication channels to a communication network that can carry many communication channels. The network communication media may consist of optical fiber and/or microwave radio. The network topology usually has several communication nodes, where channels are inserted or dropped, and may be looped to provide alternate paths if one segment of the network fails or is taken out of service for maintenance.

Relay-to-relay logic communication is interfaced to the network communication multiplexer through an EIA-232 card inserted in the multiplexer rack as shown in Figure 16. The relay serial communication port is connected to the EIA-232 multiplexer interface card with a shielded metallic cable or a fiber-optic cable with fiber-optic transceivers. Fiber-optic communication is recommended between the relay and the multiplexer to eliminate any effect of electrical interference from the substation environment.

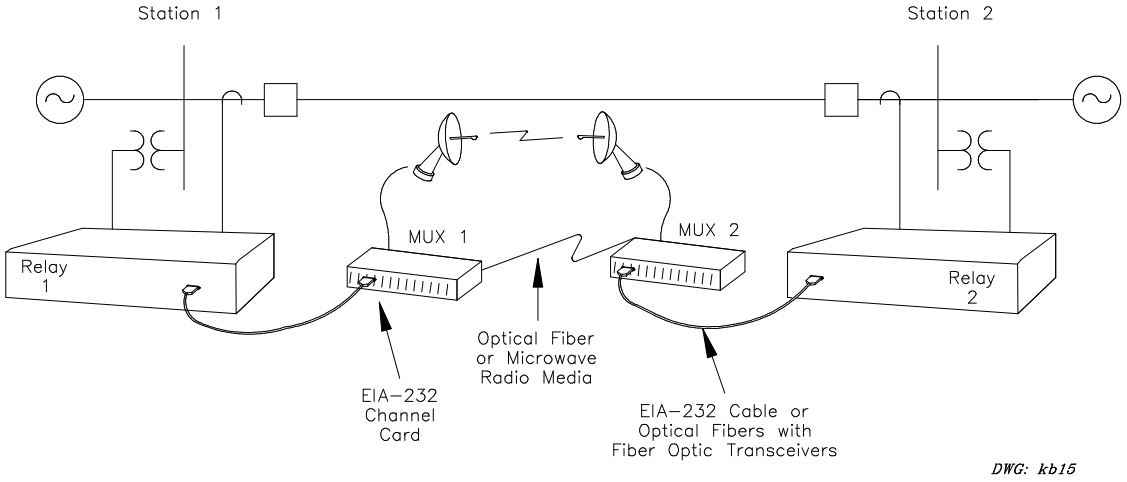


Figure 16: Digital Communication via Network Communication Multiplexers

Network administration, such as channel addressing and synchronizing are handled in the network multiplexer. Some network multiplexers also perform error checking. If the channel goes down due to failure or data error, the network multiplexers must “re-synchronize” the signal communication path before the communication channel is restored. This re-synch time depends on the type of multiplexer equipment and “switching” technique used. The simplest switching techniques require only a few milliseconds to re-synch, where those with more complex handshaking signals may take up to 60 milliseconds to re-synchronize.

Network multiplexers that perform error detection may cause data delays that affect the end-to-end relay logic response time. Check with the communication equipment manufacturer for information about data delay.

Digital Communication via Point-to-Point Digital Radio

Point-to-point digital radio provides stand-alone communication between two sites. Radios are available that operate in the 900 MHz frequency band with relatively low power ratings that may

not require special licensing, and have a range of around 20 to 30 miles, with line-of-site operation. The radios include an EIA-232 transceiver to interface with the relay EIA-232 serial communication port at rates up to 9,600 baud.

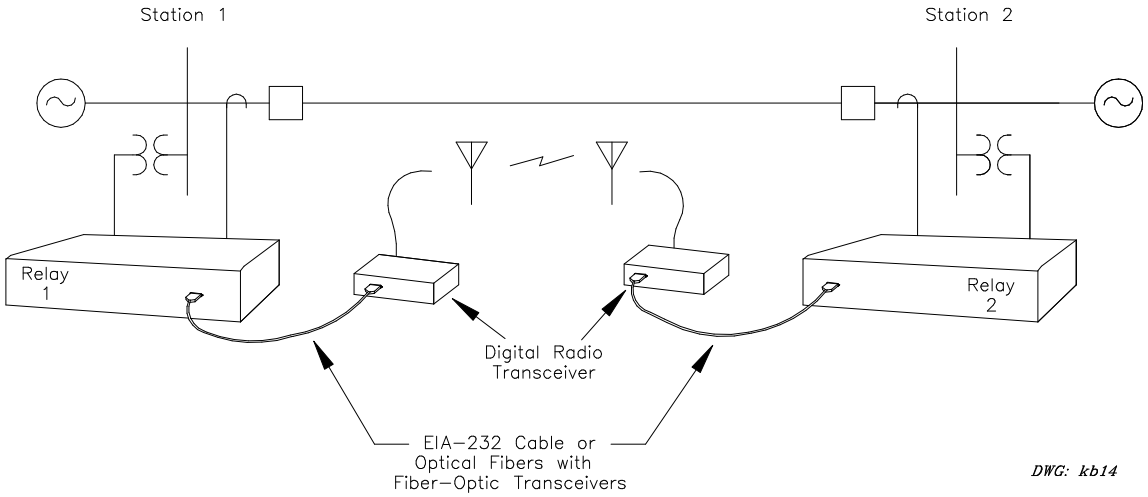


Figure 17: Digital Communication via Point-to-Point Digital Radio

Radios with no built-in error detection work best with relay-to-relay logic communication because they add only two or three milliseconds to the overall relay-to-relay communication data delay. Those radios that have built-in error detection may introduce data delays of 60 milliseconds or more. Because speed is a very critical aspect of most pilot communication schemes, be sure to check the radio specifications carefully for the radio system data delay characteristics.

Digital Communication via Leased Digital Communication Channel

Editorial Note: This application is no longer recommended by Schweitzer Engineering Laboratories, Inc., please contact the factory for more details.

Another relay-to-relay communication alternative is to lease a dedicated digital communication channel from a local service provider (telephone company). The dedicated digital communication channel is typically supplied in the form of a four-wire metallic communication circuit from the nearest central office, similar to an analog communication channel. The digital communication channel, referred to as a DS0 channel, has 56 kilobits-per-second communication capability, which is more than sufficient for the 9,600 or 19,200 baud serial communication rate on the relay.

The relay serial communication port is interfaced with the leased digital communication channel through a digital service access device called a Channel Service Unit/Data Service Unit (CSU/DSU) in North America or Line Terminating Unit (LTU) in Europe. Digital service access devices perform two functions. The digital interface to the customer's equipment (EIA-232 in this case) is provided by the DSU portion of the unit, and the interface to the digital transmission circuit, including line conditioning and equalization, is provided by the CSU portion of the unit.

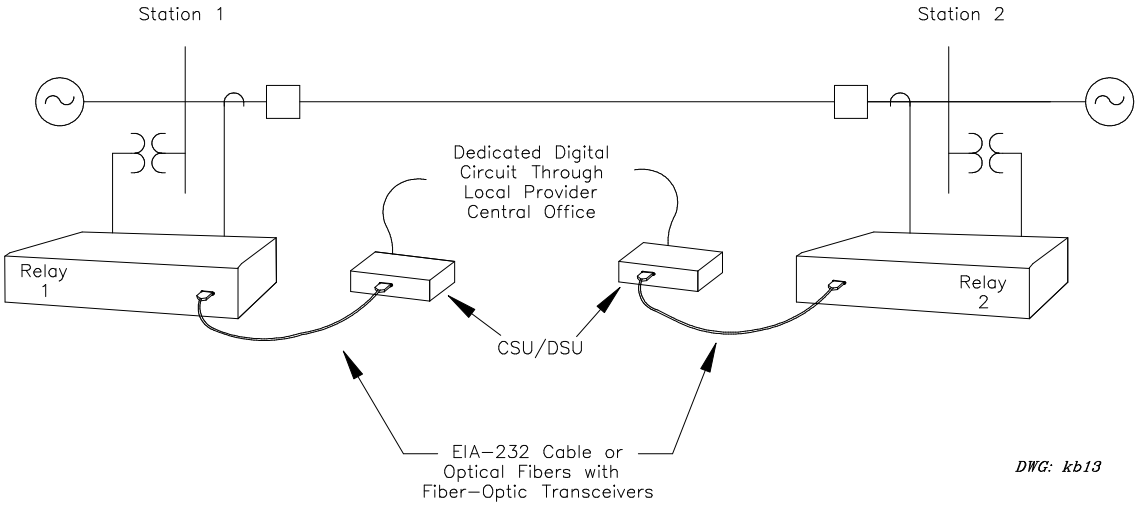


Figure 18: Digital Communication via a Leased Digital Communication Channel

Data delay through the CSU/DSU and leased digital circuit is insignificant, provided there is no error detection/correction performed outside the relay. Check with your CSU/DSU vendor and digital circuit service provider about data delay characteristics.

The dedicated digital circuit, leased from a local service provider, is routed through at least one central office. If the substations are located in different central office territories, the circuit will be routed through multiple central offices, in which case the service provider may multiplex the circuit on a communication network. As discussed earlier, path switching in networks can momentarily disrupt communication. Check with your local service provider about data delay and circuit switching.

Digital Communication via Analog Communication Channels

Editorial Note: This application is no longer recommended by Schweitzer Engineering Laboratories, Inc., please contact the factory for more details.

Leased analog communication circuits are commonly used for traditional pilot communication schemes. They can also be applied to the new relay-to-relay logic communication scheme by simply connecting the selected serial communication port on each relay to the analog communication circuit via a leased-line modem. The dedicated analog communication channel is typically supplied in the form of a four-wire metallic communication circuit from the nearest service provider's central office. The leased-line modem, much like the CSU/DSU for leased digital circuits, interfaces with the relay's EIA-232 serial port and provides line conditioning and equalization on the interface with the analog communication circuit.

Unlike the dial-up modem, the leased-line modem is connected all of the time, listening for a carrier signal that indicates that the remote-end modem is operational. Data transfer can occur as soon as both modems go "off-hook" and a data connection is established.

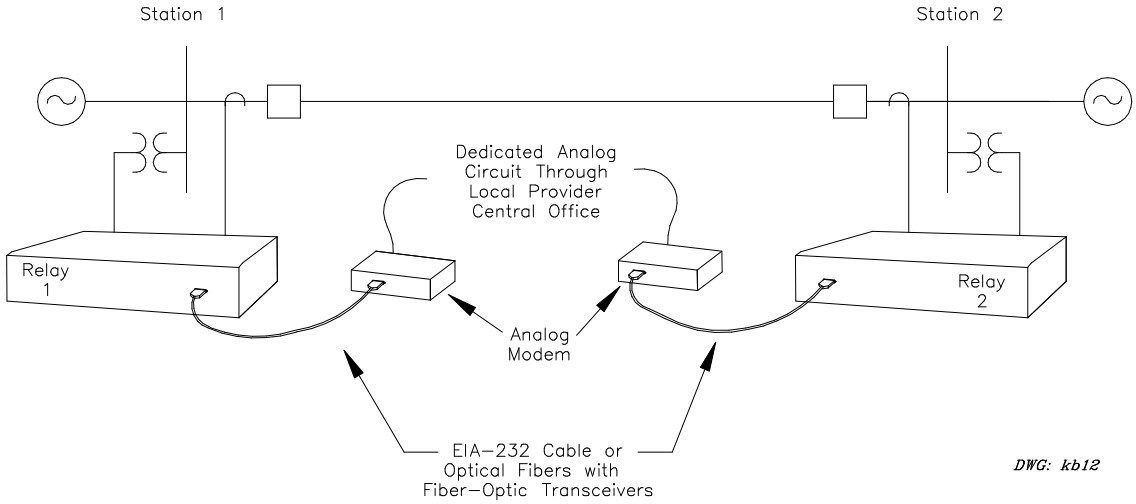


Figure 19: Digital Communication via a Leased Analog Communication Channel

Typical voice-grade analog circuits have a frequency bandwidth of about 300 to 3,000 Hz. In a full duplex communication system, about half of the bandwidth is used for communication in each direction. With a one-to-one relationship between bandwidth and baud rate, this limited bandwidth permits analog modems to transmit at communication rates up to 1,200 baud without data compression.

Above 1,200 baud, modems must apply some form of data compression. While data compression improves the modems overall data throughput, it makes the modem more sensitive to channel noise and introduces data delay in the transmitted signal. Increased sensitivity to channel noise dictates that the modem incorporate data error detection, and some “smart” modems incorporate error correction. All of this requires data buffering, which further increases the data delay. Because of the emphasis on data throughput in today’s communication market, it is difficult to find modems that do not have “smart” features that increase the data delay.

Consequently, relay-to-relay logic communication via analog communication tends to incur a higher data delay than digital communication channels.

Direct Digital Communication via Metallic Cable

Direct digital relay-to-relay logic communication via metallic cable encounters the same pitfalls as our ideal direct-connected pilot communication channel discussed earlier. Ground potential rise and induced voltages and currents make a direct metallic connection between relays susceptible to electrical interference which creates a personnel hazard. It is, therefore, not recommended for pilot scheme communication applications.

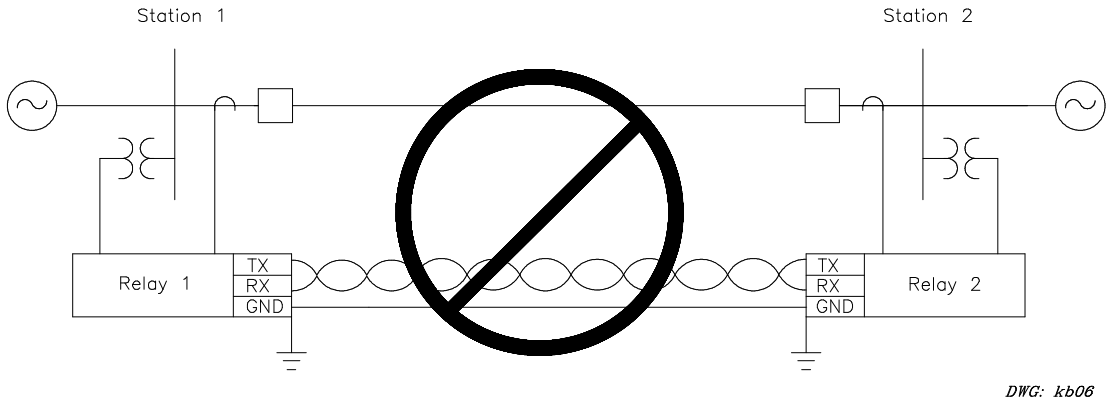


Figure 20: Direct Digital Communication via Metallic Cable - Not Recommended for Pilot Scheme Communication

CONCLUSION

In this paper, we discuss a new, innovative approach to perform pilot communication scheme functions between microprocessor-based relays at different substations. The new approach capitalizes on the communication capability built into modern microprocessor-based relays, eliminating the need for the separate traditional pilot communication equipment. The new approach provides fast, secure, and dependable communication for up to eight independent protection, monitoring, and control functions.

The paper also discusses the communication channel considerations for relay-to-relay logic communication. This new communication approach can be applied to any communication channel capable of communicating a digital message, including direct optical fiber, multiplexed optical fiber and/or microwave radio, direct point-to-point radio, and leased analog or digital circuits.

REFERENCES

1. IEC 834-1, “Performance and Testing of Teleprotection Equipment of Power Systems,” Draft 31, July 1995.

2. IEEE/PSRC, “Inter Substation Protection Using Digital Communications,” Draft #8.

APPENDIX A: MATHCAD PROGRAM TO CALCULATE RELAY-TO-RELAY LOGIC COMMUNICATION CHANNEL SECURITY AND DEPENDABILITY

Ken Behrendt
July 30, 1996

SECURITY CALCULATIONS FOR A DIGITAL CHANNEL

Security is a measure of the probability that all corrupted messages will be detected and rejected so they do not cause an unwanted action. A perfectly secure channel produces no unwanted action. The probability that a corrupted message escapes detection by the relay security checks is PK, so the channel security, PS, is 1-PK.

Calculate the probability (PK) that a corrupted message will go undetected by an error detection scheme consisting of a 6-bit CRC looking at eight data bits, and two flag bits that identify the proper word sequence in the message:

Where: $Z := 1 \ldots 9$

$P_Z := 10^{-Z}$ P = Bit Error Rate (BER) of the channel

$CRC \equiv 6$ CRC = Number of CRC bits

$N \equiv 8$ N = Number of bits checked by the CRC

$K \equiv 4$ K = Minimum number of bits where the CRC is not 100% effective in detecting errors (hamming distance)

$$PKCR_Z := \left[\frac{2}{70}\cdot\left(P_Z\right)^K\cdot\left(1-P_Z\right)^{(N-K)}\right]+\left[\frac{1}{32}\cdot\left(P_Z\right)^K\cdot\left(1-P_Z\right)^{(CRC+N-K)}\right]$$

Probability that the CRC bit calculation will not detect a corrupted message.

$PKFB_Z := (1-P_Z)^2$ Probability that the flag bits will not detect a corrupted message.

$PK_Z := (PKFB_Z)\cdot(PKCRC_Z)$ Combined probability that a corrupted message will pass undetected.

$PS_Z := 1-PK_Z$ Probability that the channel is secure.

P_Z	PK_Z	PS_Z
$1 \cdot 10^{-1}$	$2.4 \cdot 10^{-6}$	0.999997599004841
$1 \cdot 10^{-2}$	$5.5 \cdot 10^{-10}$	0.999999999454010
$1 \cdot 10^{-3}$	0	0.999999999999941
$1 \cdot 10^{-4}$	0	1.000000000000000
$1 \cdot 10^{-5}$	0	1.000000000000000
$1 \cdot 10^{-6}$	0	1.000000000000000
$1 \cdot 10^{-7}$	0	1.000000000000000
$1 \cdot 10^{-8}$	0	1.000000000000000
$1 \cdot 10^{-9}$	0	1.000000000000000

The results show that the combination of 6-bit CRC and byte flags provide extremely high message security over a wide range

Dependability Calculations for a Digital Channel

Dependability is a measure of the probability that a transmitted message will be received. Assuming the relay detects and rejects every bad message, and rejects an additional six good messages that follow the bad message, we can calculate the Missing Message Rate, MMR, which is the number of rejected messages per message sent. This is a conservative calculation that assumes that only one corrupt bit occurs within each corrupt message.

The probable channel dependability, PD, which is the number of good messages received per message sent, is calculated by the equation: PD = 1-MMR.

$MER_Z := P_Z \cdot 20$ — For every error bit sent, there is one bad message. For every message, there are 20 bits sent, so the Message Error Rate (MER) is the Bit Error Rate (BER) * 20.

$MMR_Z := MER_Z \cdot (1 + 6)$ — Missing Message Rate (MMR) is the Message Error Rate times (1+6) because for every corrupt message detected, the relay rejects the next six good messages.

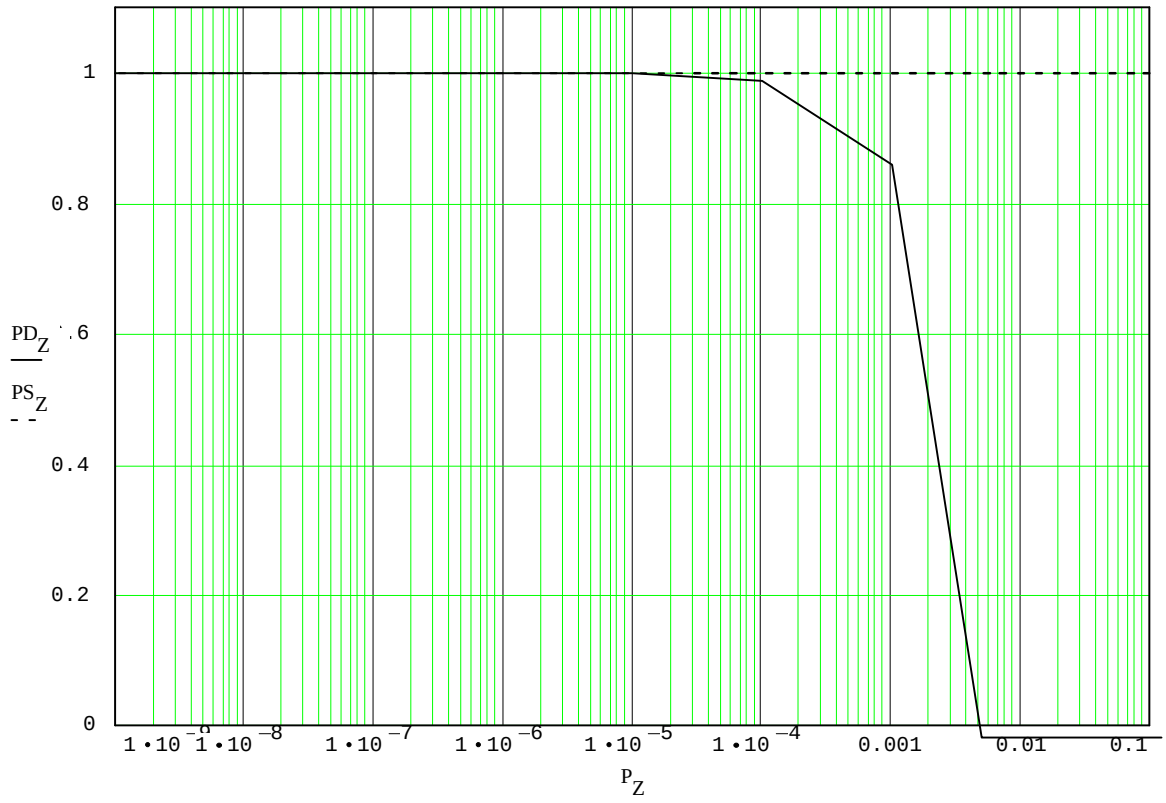
$PD_Z := 1 - MMR_Z$ — Dependability is the Message Transmission Rate (1) less the Missing Message Rate.

P_Z	MMR_Z	PD_Z
$1 \cdot 10^{-1}$	$1.4 \cdot 10$	-13.000000000
$1 \cdot 10^{-2}$	1.4	-0.4000000000
$1 \cdot 10^{-3}$	0.1	0.86000000000
$1 \cdot 10^{-4}$	$1.4 \cdot 10^{-2}$	0.98600000000
$1 \cdot 10^{-5}$	$1.4 \cdot 10^{-3}$	0.99860000000
$1 \cdot 10^{-6}$	$1.4 \cdot 10^{-4}$	0.99986000000
$1 \cdot 10^{-7}$	$1.4 \cdot 10^{-5}$	0.99998600000
$1 \cdot 10^{-8}$	$1.4 \cdot 10^{-6}$	0.99999860000
$1 \cdot 10^{-9}$	$1.4 \cdot 10^{-7}$	0.99999986000

These results indicate that the dependability falls to zero (or less) when every seventh message is corrupt, and the dependability approaches 1 when the channel BER is less than 1 per 10 000 bits

Security and Dependability vs. Bit Error Rate

The X-Y plot shows the relationship between relay-to-relay logic communication channel security, PS, and channel dependability, PD, over a channel bit error rate range.



APPENDIX B: PROBABILITY OF A MISDETECTION USING A 6-BIT CRC

Jian Chen, Jeff Roberts, and Ken Behrendt
July 30, 1996

We can prepare a message for transmission over a digital communications channel by first expressing this message as a binary sequence. After the message is converted to a binary sequence, we can then issue it to a serial port for communication transmission. Because this message is a sequence of two-state bits (either 1's or 0's), we must concern ourselves with the validity of the received message. A message error occurs if 1 or more of the message bits flip (0 to 1 or 1 to 0) during transmission. It is easier to flip one bit than two or more bits. That is, the further the hamming distance between two binary sequences x and y, the harder it is to receive y when x is transmitted.

Definition: *The hamming distance between two binary sequences, x and y, is the number of places in which they differ.*

For example, the hamming distance between the x and y messages shown below are (in ascending order of hamming distance):

x = 10101000
y = 11111000
01010000 - - the hamming distance is 2

x = 10101000
y = 10010000
00111000 - - the hamming distance is 3

x = 10101000
y = 01110000
11011000 - - the hamming distance is 4

Let's next look at the relay-to-relay logic communication implementation.

- 8-bit message field, the number of different messages $= 2^8 = 256$,
- 6-bit CRC field, the number of different CRC possibilities $= 2^6 = 64$.

For the 8-bit message and the 6-bit CRC, the number of messages with the same CRC is 4 ($2^8/2^6 = 256/64 = 4$). This means that four different 8-bit messages share the same CRC. Put another way, for every 8-bit message sent, there are four out of 256 messages that will generate exactly the same CRC. If the transmitted message flips into any of the three other messages with the same CRC, a misdetection occurs (i.e., the flawed message is not detected by the CRC check).

How hard is it to send a message which flips into one of the other possible three 8-bit combinations with the same CRC? How hard (or how easy) it is depends on the minimum hamming distance between the four same-CRC messages. The greater the hamming distance between these same-CRC messages, the lesser the probability of this misdetection occurring.

The generator polynomial for a 6-bit CRC is:

$$g(x) = x^6 + x^5 + x + 1$$

and generates the following codes:

Message #	***message bits***	***CRC bits***	***hamming distance***
1	00000000	000000	message sent
2	01100101	000000	4*
3	10101111	000000	6
4	11001010	000000	4*
1	00110010	000001	message sent
2	01010111	000001	4*
3	10011101	000001	6
4	11111000	000001	4*
1	00011001	000010	message sent
2	01111100	000010	4*
3	10110110	000010	6
4	11010011	000010	4*
1	00101011	000011	message sent
	. . .	. . .	

Using a 6-bit CRC, we see from the above table that the minimum hamming distance between the same-CRC messages is four, and the number of messages with the same CRC is four.

Let's assume that the channel bit error rate (BER) is p. The probability of one bit flipped is p, two bits flipped is p^2 , three bits flipped is p^3, and four bits flipped is p^4 . Remember that the minimum hamming distance is four bits. Therefore, the probability of a misdetection is some factor multiple of p^4. Using a 6-bit CRC then reduces the probability of misdetection to some factor multiple of p^4.

The probability of a misdetection, P*md*, for the 6-bit CRC is expressed in the form:

$$Pmd \approx \frac{A}{B} p^K (1-p)^{N-K} \qquad \text{Equation 1}$$

where:

A is number of minimum hamming distance occurrences per common CRC group
B is the total number of CRC groups with the minimum hamming distance
N is the number of bits in the transmitted message checked by the CRC
K is the minimum number of bits where the CRC is not 100% effective
p is the channel bit error rate

We use an approximation because the total probability calculation is a series. However, the first term of the series dominates the results, so we use only the first term to simplify the calculations.

The fourth column in the table above indicates that there are two (2) each hamming distance-4 messages in each same-CRC group, and there are a total of 70 hamming distance-4 messages in the 8-bit message field (complete table not shown). Now we can write the probability of a misdetection (p_{md}) as:

$$Pmd \approx \frac{2}{70} p^4 (1-p)^4 \qquad \text{Equation 2}$$

Another case that can lead to a misdetection is that both message and transmitted CRC flip during transmission: the message flips from CRC-group one to CRC-group two and the CRC flips from CRC one to CRC two. Considering both the message and CRC flipping, we can calculate the probability of a misdetection as:

$$Pmd \approx \frac{2}{70} p^4 (1-p)^4 + \frac{1}{32} p^4 (1-p)^{10} \qquad \text{Equation 3}$$

Effect of Byte Flags on Error Detection

Let's look next at the effect of byte flags on error detection as there are two flag bits in the transmitted *Mirrored Bit* message. These flag bits act as a filter as the rest of the message is not even considered unless the flag bits are correct. Considering the flag bits, the probability of a misdetection becomes:

$$Pmd \approx (1-p)^2 \left[\frac{2}{70} p^4 (1-p)^4 + \frac{1}{32} p^4 (1-p)^{10} \right] \qquad \text{Equation 4}$$

As the value of (1-p) is very nearly 1, including the flag bits does not significantly improve P_{md} . This is not to say that byte flags are unnecessary because they are needed for byte sequence identification; i.e., identifying if it is the first or second byte of the transmitted mirror bit message.

Years/Errorword Calculations for a 6-bit CRC

What does this probability tell us? Let's assume we have a relatively poor channel with the following communication characteristics:

- the BER is 10^{-4}. i.e. $p = 10^{-4}$, and $P_{md} = 5.98 \cdot 10^{-18}$ errorword/word
- the data rate is 9600 bits/sec. 960 bytes/sec, 480 word/sec

From this information, we can calculate how often we can expect that a corrupted message will escape detection by message security checks. The calculation technique is as follows:

$$\text{Time(errorword / sec} = \frac{10^{18} \text{ word}}{5.98 \text{ errorword}} \text{ x } \frac{1 \text{ sec}}{480 \text{ word}} = 3.5 \text{ x } 10^{14} \frac{\text{sec}}{\text{errorword}}$$

That is:

$3.5 \cdot 10^{14}$ sec/errorword = $9.7 \cdot 10^{10}$ hours/errorword
= $4 \cdot 10^{9}$ days/errorword
= 10,958,904 yrs/errorword

This means that once in nearly 11 million years, we could expect to experience a misdetection!

981117 Printed in USA