Multiapplication Ethernet in IEDs – Processing, Connection, and Integration Issues

Roy Moxley and Bob Morris
Schweitzer Engineering Laboratories, Inc.

Published in the
proceedings of the 3rd Annual Protection, Automation and Control World Conference
Budapest, Hungary
June 25–28, 2012

Originally presented at the
14th Annual Western Power Delivery Automation Conference, March 2012

Multiapplication Ethernet in IEDs – Processing, Connection, and Integration Issues

Roy Moxley and Bob Morris, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Serial ports on intelligent electronic devices (IEDs) had the initial advantage of being used for a single application: engineering access, supervisory control and data acquisition (SCADA) connections, event reporting, or device-to-device signaling. Interleaved messages were added to some devices, which enabled additional control signals and metering data to be sent over the same channel and at the same time as engineering access.**

While different IEDs have different functions available for automation and integration, a major difference between serial and Ethernet ports is that these multiple functions may be performed on the same Ethernet port. Automation capabilities in IEDs increase with the use of Ethernet connections, but the connection and processing complexities increase also.

A single IED can have multiple applications, such as wide-area measurements, IEC 61850 MMS messages, IEC 61850 GOOSE, DNP3 messages to SCADA, and engineering access file transfer and Telnet, all going on at the same time. Future applications could require all of those plus Precision Time Protocol (PTP, IEEE 1588) time signals and IEC 61850-9-2 voltage and current signals.

These signals must be processed within the IED, and the network connecting to the IED needs appropriate security and dependability. This paper discusses the processing considerations (within the IED) of Ethernet messages and network bandwidth requirements. Routing considerations are discussed to assist automation engineers in assessing specific application suitability. The impact of message load on IED processing is presented with conclusions on ensuring proper scheme operation.

I. Introduction

Automation systems are all about communicating information from device to device throughout the system and from system devices back to a central location. The central location may be at a substation or at a headquarters location. The different function of the various messages sent to different locations also means that different reliability, security, and speed requirements are indicated. For example, consider a system like the one shown in Fig. 1.

Fig. 1 illustrates, from a functional standpoint, a typical and reasonable set of communications to and from a modern protective relay. The speed, security, and reliability requirements of each of the signals are different and depend on the use of the information sent and received. Speed requirements are measured from the time a signal is sent from the local relay to the receipt of that signal at the remote device. Security is defined, in this paper, as the ability of the receiving device to detect corrupted messages and take appropriate action. Reliability is defined as the signal getting through to the receiver uncorrupted. By looking at the communications requirements of each application, we gain insight into the final system configuration requirements.

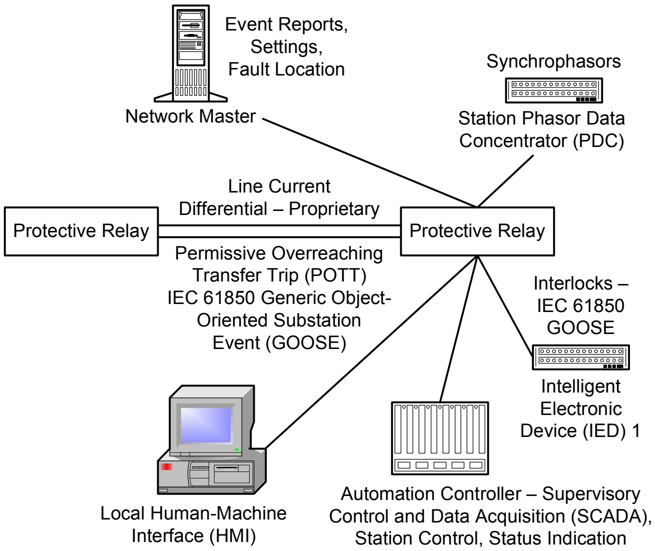

Fig. 1. Communications from an individual protective relay

Communications requirements and path capabilities lead to application questions for the automation engineer. How are these differences managed in order to meet the application requirements? What are the limitations of different devices along the communications path that can impact application performance? These questions must be addressed in order to ensure the overall automation system (possibly including high-speed protection and control) functions to the system requirements.

II. Path Considerations

Of course, the communications as shown in Fig. 1 are not a reasonable description of physical connections. The seven connections to the relay are probably beyond what would be desirable (or possible) in a real protective relay. An obvious answer to this problem is to use Ethernet connections to multiplex applications. This simplifies the relay connections to the system shown in Fig. 2.

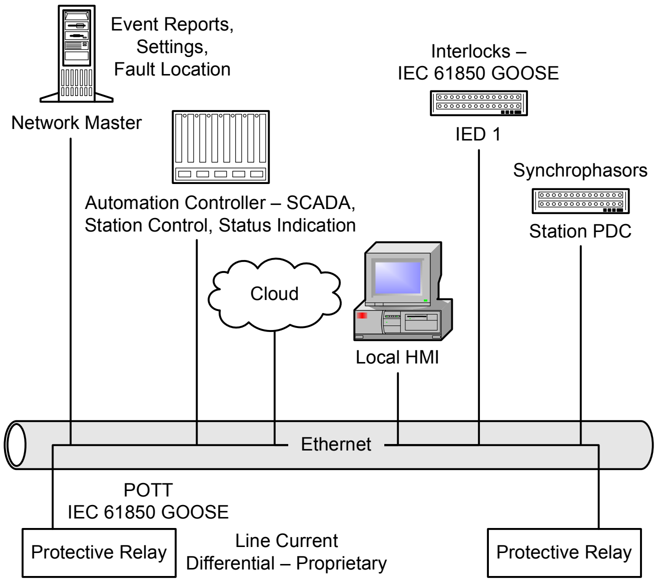

Fig. 2. Communications from a relay using an Ethernet connection

Now, instead of seven connections to the relay, we only have one. Of course, the Ethernet system must handle the variety of requirements shown in Table I.

TABLE I
SPEED, SECURITY, AND RELIABILITY REQUIREMENTS OF DIFFERENT INFORMATION FUNCTIONS

Function	Speed Requirement	Security Requirement	Reliability Requirement
Event reports	Low	Medium	Medium
Remote settings	Low	High	Medium
Fault location	Low	Low	Low
Line current differential	High	High	High
POTT	High	High	High
Local HMI	Low	Medium	Medium
Station automation – SCADA, station control, status	Medium	High	Medium
Interlocking	High	High	High
Synchrophasors	Medium	Medium	Medium

III. Relay Processing Considerations

While some of the functions shown in Fig. 2 (such as HMI, SCADA, and event reports) can be done in the background (at lower speeds than every processing interval), others must be performed at high speed. Interlocks, POTT, and critical automation applications require protective relays to process data from remote devices at high speeds. Tests using the test setup shown in Fig. 3 were performed on a number of different devices [1].

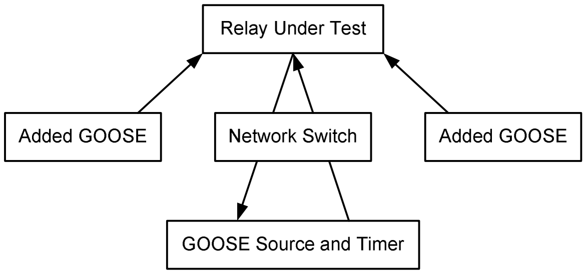

Fig. 3. GOOSE performance test setup

As seen in Fig. 4, these tests show that most relays have good performance on Ethernet communications systems with light loading of the communications port.

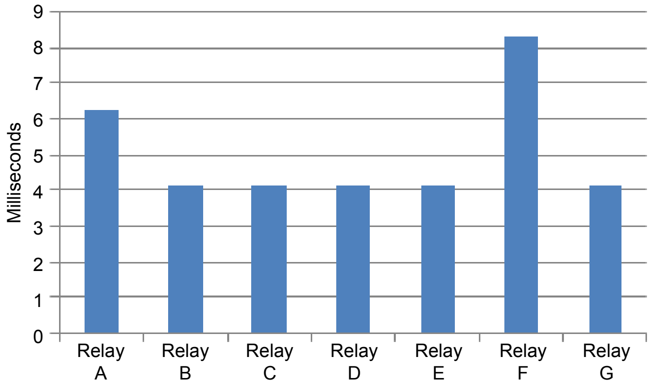

Fig. 4. Relay-to-relay data transfer time (low traffic)

The time indicated is to receive an IEC 61850 GOOSE message from one relay and then produce an output response GOOSE message back to the source. Output contact speed is not considered in the Fig. 4 graph. These speeds are sufficient for any of the applications shown in Table I, including current differential.

These speeds are in an unloaded network. Depending on how the station network is configured, we could reasonably expect that during a system event, such as a line fault, there would be a large number of extra messages being sent and received on the network. It is recognized that setting virtual local-area network (VLAN) priority on messages can help reduce this congestion. However, even with proper VLAN priorities, a large-packet, low-priority message can still create large and difficult-to-predict queuing or processing delays for other higher-priority traffic [2].

This was demonstrated in congestion testing of the same Fig. 4 relays. The test setup was similar, but additional IEDs were used to inject other GOOSE messages onto the network. The results of this test are shown in Fig. 5.

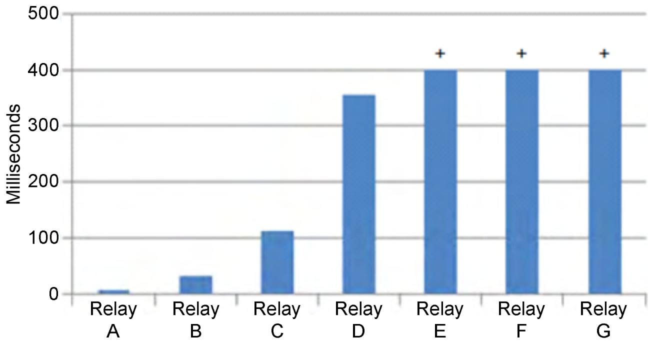

Fig. 5. Relay-to-relay data transfer time with two subscribed and four unsubscribed messages

The significant item from Fig. 5, regarding this paper, is that these times are not a result of congestion on the network. These delays were the result of congestion within the relays connecting to the network. While it is important to properly control messages on the network to avoid a relay being subject to unsubscribed messages, this does not address the legitimate messages that are being sent to the relay. The relay under test was only subjected to seven total GOOSE messages, not an unrealistic number for many applications. Also, it is important to note that the performance of the device at low message levels was not a predictor of its performance at high message rates.

Consider the performance of Relay A in the test shown in Fig. 4. When the number of messages hitting the relay port increased, its speed remained the same. This was in marked contrast to other relays that suffered considerable degradation of performance as the port was exposed to increased messages.

The different types of signals detailed in Table I are frequently combined within a single relay. For example, a relay-to-relay signal could be between one relay and multiple other relays. Consider a simple station, as shown in Fig. 6.

It would be reasonable for the source relays (shown on the left in Fig. 6) to receive coordination (blocking) signals from each feeder relay, as well as breaker failure signals, source throw-over signals, and other specialized station control signals. This would be in addition to the synchrophasor, SCADA, HMI, and other types of signals in Table I. It would not take a very large station before the conditions of the test shown in Fig. 5 are reached.

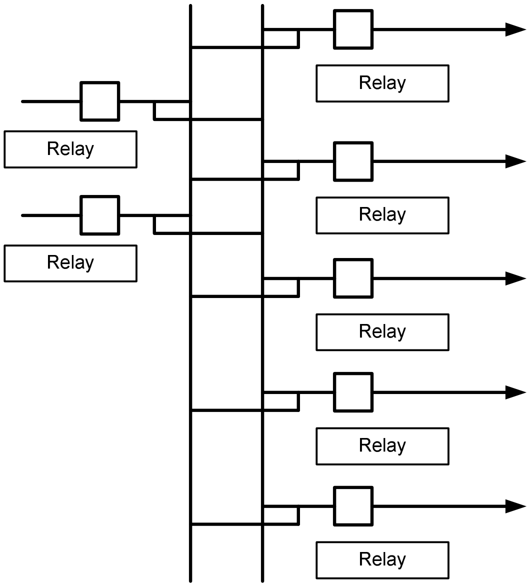

Fig. 6. General station with feeder (right) and source (left) relays

The first level of defense for a flood of high-priority messages is to segregate traffic within a port. As shown in Fig. 7, specialized hardware within the relay can be used to filter the GOOSE traffic based on addressing before it reaches the microcontroller.

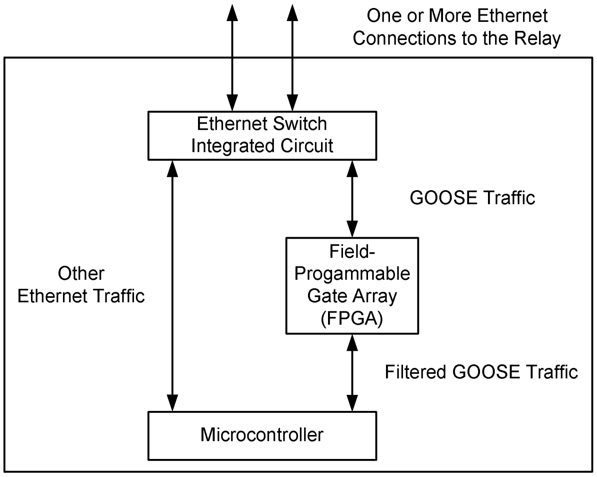
One or More Ethernet Connections to the Relay
Ethernet Switch Integrated Circuit
GOOSE Traffic
Other Ethernet Traffic
Field-Progammable Gate Array (FPGA)
Filtered GOOSE Traffic
Microcontroller

Fig. 7. GOOSE message segregation prior to processing

The GOOSE filter inside the FPGA is designed to pass only GOOSE messages to which the relay has subscribed on to the microcontroller. In a system with this type of filtering, no processing time is used by the relay on unsubscribed messages. This improves the response speed for high-priority messages. Lower-priority inbound and outbound messages use a separate path within the relay and may be merged into a single path near the external connectors using an embedded Ethernet switch.

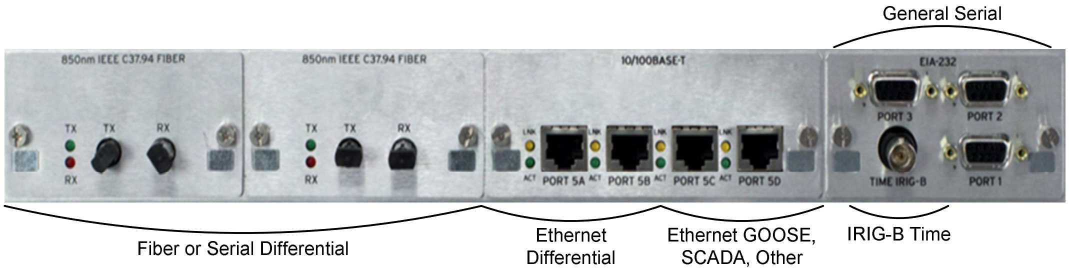

Fig. 8. Communications ports on an advanced protection and control device

IV. Communications Ports

Preventing port congestion by increasing the number and type of ports in a device is another way of avoiding communications congestion problems. Using different physical ports for different functions, or classes of functions, avoids overloading processes in the device. While older protection and control devices may have had only a few serial ports and one Ethernet port, more modern devices give a designer a broader selection. For some devices, the choice has been to bring current transformers, voltage transformers, contact inputs, and contact outputs into the relay in digital form over a custom cable [3]. While this approach addresses some communications issues from the circuit breaker cabinet, the transmission of information between devices remains an issue.

Consider a view of communications ports on a device, as shown in Fig. 8. Note that in this case, there are numerous ports that have the same potential function as other ports. The differential communications can be over either a traditional serial interface (fiber or EIA-422 multiplexed) or over an Ethernet port. SCADA can be over an Ethernet port (such as DNP3 over Ethernet) or a traditional serial port. Time distribution can be over a traditional IRIG-B port or use Ethernet Simple Network Time Protocol (SNTP) or, in the future, IEEE 1588 Precision Time Protocol (PTP) time distribution.

The choice of which system and port to use is not always a matter of convenience. Time distribution with SNTP is only accurate to about 5 milliseconds. This is enough accuracy for many fault analysis applications [4], but for closely timed events, this may be insufficient to determine cause and effect. For synchrophasors and clock-based synchronization of differential signals, this level of accuracy is clearly insufficient. When IEEE 1588 PTP time distribution systems become widely established, there could be accurate Ethernet time distribution.

The application of Ethernet differential communications is new in the industry. The critical nature of communications to differential relays is well known [5]. In order to avoid adding complexity to the data synchronization process when using Ethernet for differential communications, the left two Ethernet ports in the example relay of Fig. 8 are used exclusively for differential. The right two Ethernet ports are used for all other Ethernet communications, including IEC 61850 GOOSE. This is very important both for the differential signal and GOOSE messages. Consider a differential relay experiencing degradation in communications speed, as shown in Fig. 5. A delay of 100 milliseconds would add a possibly intolerable tripping delay for internal faults and a loss of security for external faults.

Port segregation of functions prevents one set of critical communications from interfering with another.

V. Network Solutions

Network solutions can reduce communications problems to individual relays. For example, VLANs between communications nodes restrict message traffic from reaching unaddressed devices, as shown in Fig. 9 [1].

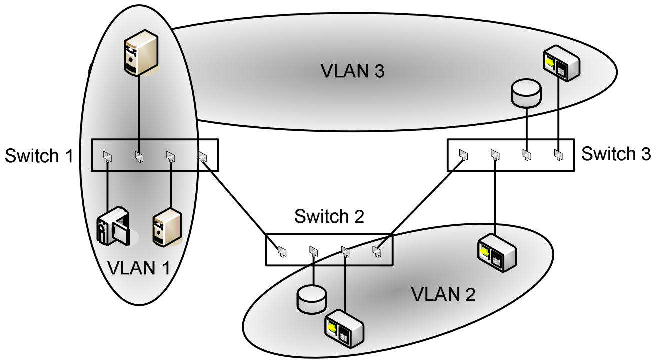

Fig. 9. Switched Ethernet and VLAN configuration

Notice that traffic can be isolated between devices by setting up appropriate VLANs. In Fig. 9, traffic at devices connected to VLAN 3 will not reach devices on Switch 2 or devices on Switch 1 or Switch 3 that are not part of the VLAN. This can be further refined by using an Ethernet-over-SONET (synchronous optical network) multiplexer system. Applying differential communications to one Ethernet channel and other Ethernet communications (GOOSE, synchrophasors, and so on) to other channels prevents overburdening of one port.

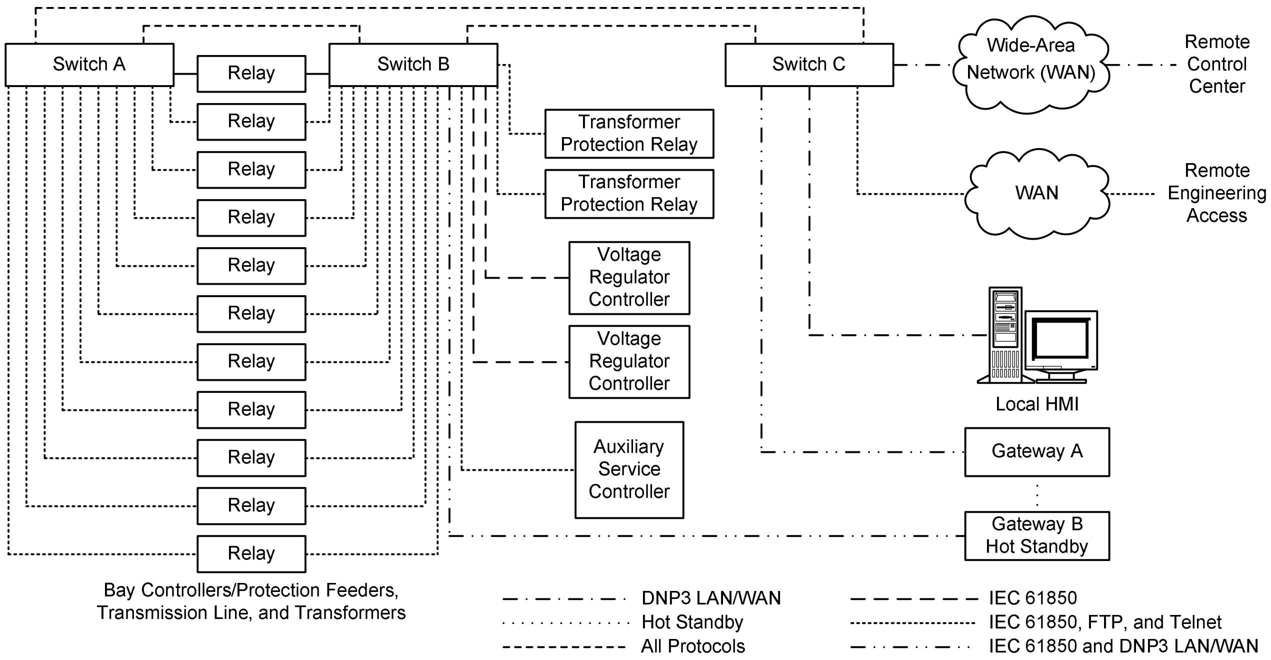
Switch A
Relay
Relay
Relay
Relay
Relay
Relay
Relay
Relay
Relay
Relay
Relay
Switch B
Transformer Protection Relay
Transformer Protection Relay
Voltage Regulator Controller
Voltage Regulator Controller
Auxiliary Service Controller
Switch C
Wide-Area Network (WAN)
Remote Control Center
WAN
Remote Engineering Access
Local HMI
Gateway A
Gateway B Hot Standby
Bay Controllers/Protection Feeders, Transmission Line, and Transformers
DNP3 LAN/WAN
Hot Standby
All Protocols
IEC 61850
IEC 61850, FTP, and Telnet
IEC 61850 and DNP3 LAN/WAN

Fig. 10. Network architecture adopted for an automation system

The diagram in Fig. 9 shows only one network path between the various devices and switches. An example of the path connections used in an actual station is shown in Fig. 10 [6].

Note that in this application, every relay and every switch has two connections. There is even a hot standby station gateway. In this way, the failure of a single component (port on a relay, port or individual switch, and station gateway) cannot cause the loss of any information or function. This type of connection is well known to relay and control engineers as it is applied to the overall relay scheme, with Main 1, Main 2, and backup protection.

VI. Conclusion

Communications of internal relay data to other relays, station devices, and central location systems are a fact of life in modern protection, control, and automation schemes. This paper demonstrates the need for communications system management and the consequences of a failure to manage data flow at the relay location, including the following:

- Ethernet communication can provide diverse signals to and from a relay or control device, including time, line differential, IEC 61850 digital and analog messages, SCADA, HMI, and other information.
- Combining all Ethernet messages on a single port can cause noncritical data to delay critical protection and control processes.
- Most delays in Ethernet communications within a station are due to data processing limitations in the IED, not the network.
- Advanced devices offer the option to separate signals onto a variety of ports, including Ethernet and serial.
- All communications ports on a station IED should have failover or dual-path capabilities to improve reliability.

Just as the use of wiring for connecting devices requires thought and care, so the use of digital and especially multifunction communications ports requires thought and care. By properly selecting port and communications system architecture, protection and control reliability and security are improved and enhanced.

VII. References

[1] K. Leggett, R. Moxley, and D. Dolezilek, “Station Device and Network Communications Performance During System Stress Conditions,” proceedings of the Protection, Automation and Control World Conference, Dublin, Ireland, June 2010.

[2] T. S. Sidhu, M. G. Kanabar, and M. R. Dadash Zadeh, “IEC 61850-9-2 Based Process Bus,” *PAC World Magazine*, December 2010. Available: http://www.pacw.org/issue/december_2010_issue/process_bus/iec_6185092_based_process_bus/article/3.html.

[3] M. Adamiak, J. C. Medina, M. Goraj, and A. Hamze, “Reducing Conventional Copper Signaling in High Voltage Substations With IEC 61850 Process Bus System,” proceedings of the 5th GCC Cigre International Conference, Riyadh, Saudi Arabia, October 2009.

[4] R. Moxley and K. Fodero, “Timing Options and Tradeoffs for Automation and Wide Area Measurement Systems – Timing Is Everything,” proceedings of the 9th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2007.

[5] B. Kasztenny, N. Fischer, K. Fodero, and A. Zvarych, “Communications and Data Synchronization for Line Current Differential Schemes,” proceedings of the 38th Annual Western Protective Relay Conference, Spokane, WA, October 2011.

[6] S. Kimura, A. Rotta, R. Abboud, R. Moraes, E. Zanirato, and J. Bahia, “Applying IEC 61850 to Real Life: Modernization Project for 30 Electrical Substations,” proceedings of the 10th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2008.

VIII. Biographies

Roy Moxley received his B.S. in electrical engineering from the University of Colorado. He joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2000 as market manager for transmission system products. Roy is now a senior product manager. He has authored and presented numerous papers at protective relay and utility conferences. Prior to joining SEL, Roy was with General Electric Company as a relay application engineer, transmission and distribution (T&D) field application engineer, and T&D account manager. He is a registered professional engineer in the state of Pennsylvania and a member of IEEE and CIGRE.

Bob Morris received his B.S. in geophysical engineering and M.S. in engineering science degrees from Montana Tech. He worked for Montana Power Company in substation and generation plant automation from 1987 to 1991. In 1991, he joined Schweitzer Engineering Laboratories, Inc. (SEL) and has held numerous positions in product design and development. He is presently a research and development director at SEL.

20120221 • TP6542-01