Deterministic Communications for Protection Applications Over Packet-Based Wide-Area Networks

Kenneth Fodero, Christopher Huntley, and Paul Robertson, *Schweitzer Engineering Laboratories, Inc.*

Abstract—**There is a growing trend in the power utility industry to move away from traditional synchronous optical network/synchronous digital hierarchy (SONET/SDH) systems for wide-area network (WAN) communications. Information technology (IT) teams and equipment manufacturers are encouraging utility communications engineers to implement Ethernet-based packet transport solutions that offer greater bandwidth efficiency. This technology migration comes with a challenge; engineers must now figure out how to design packet-based pilot channels that still meet the strict performance and determinism requirements essential for supporting protection applications. To solve this problem, this paper introduces a deterministic packet transport method for achieving guaranteed latency for critical traffic being transported over packet-based WANs that is compatible with both multiprotocol label switching (MPLS) and Carrier Ethernet systems. Latency, asymmetry, and packet delay variation (jitter) performance data are discussed to show the ability of the deterministic packet transport method to support a line current differential protection channel across mixed transport network topologies.**

I. Introduction

A typical power utility substation contains a diverse range of applications and services that rely on wide- and local-area data communications to manage the safe operation of the electric power system. Typical power utility network services include voice, teleprotection, telemetry, video, control and automation, email, and corporate local-area network (LAN) access.

Today, many protection schemes use digital communications channels. Although there are communications-assisted protection implementations that use direct, point-to-point fiber links, it has become more common to use multiplexed channels. Fodero and Robertson (2015) explained that:

> Applications with direct fiber links are simple, fast, and reliable, but they underutilize bandwidth. The move toward multiplexed channels was driven by the need to make better use of fiber assets and provide alternate fiber paths for network healing in the event of fiber breaks. Wide-area networks (WANs) are used to carry the relay protection multiplexed channels in addition to other substation services and have become an integral and necessary part of modern power network protection systems. [1]

Time-division multiplexing (TDM) has been widely adopted across the power utility industry as the preferred WAN transport technology because it provides low-latency, deterministic, and minimal-asymmetry performance. However, there is a clear trend within the industry to move toward using Ethernet and packet-based networking for all power utility applications and services, including protection. The motivation to move away from TDM-based systems is driven by a desire to converge information technology (IT) and operational technology (OT) networks and standardize on a common set of interfaces to reduce capital and operating expenses.

The migration to packet-based networking technologies such as multiprotocol label switching (MPLS) and Carrier Ethernet has created the challenge of engineering teleprotection services to provide the determinism and guaranteed performance required by protection applications. This paper proposes a method for transporting teleprotection channels across packet-based WANs while achieving the same performance as that of TDM-based systems.

II. Communications-Assisted Protection

Faults on the power system can result in disturbances, causing system and equipment damage that is costly to repair. Serious disturbances can result in large-scale blackouts and the loss of system stability [2]. Fault clearing is therefore an integral component of power transmission and distribution system design, maintenance, and operations. Protection schemes designed to identify and clear faults must meet the following objectives provided in [1]:

- Remove the faulty element from the rest of the system.
- Limit or prevent equipment damage.
- Prevent severe power swings or system instability.
- Minimize adverse effects on customer loads.
- Maintain power system transfer capability.

Communications-assisted protection schemes facilitate data sharing between protection devices and make it possible to employ methods that improve the schemes' dependability, selectivity, security, and speed. These communications-assisted schemes also enable the implementation of differential comparison schemes, such as line current differential (87L) protection. Fig. 1 shows the principle of 87L protection, where current entering a line segment is compared with current leaving the segment to determine if there is a fault. For nonfault conditions, the current going in always equals the current going out. A difference in the measured current values indicates a fault on the line, which causes the relay to initiate a breaker trip sequence.

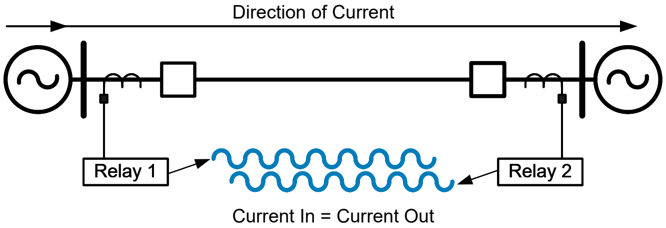

Fig. 1. 87L protection

Note that if the communications channel fails in a communications-assisted protection scheme, backup protection methods ensure that power system faults are still cleared. However, backup methods typically result in longer clearing times, causing longer fault current duration that reduces equipment life and increases the risk to personnel safety.

III. Communications Channel Performance Requirements

There are several standards that specify communications channel performance requirements for electric power substation applications. IEEE 1646, Communication Delivery Time Performance Requirements for Electric Power Substation Automation, defines a series of data delivery time requirements for different information types. These delivery times are determined by the transfer time, which is illustrated in Fig. 2 [3].

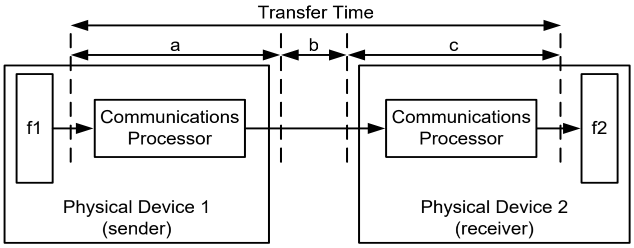

Fig. 2. Transfer time

Table I is a summary of these data transfer time requirements for line protection and control.

Table I
IEEE 1646 Communications Performance Requirements for Line Protection and Control

Data or Application	Maximum Transfer Time (ms)
Breaker tripping and breaker failure initiate	4
Backup breaker tripping (after breaker failure time-out)	8 to 12
Breaker reclosure (including voltage-supervised and multiple reclosures)	8
Control of transfer trip for send and receive commands	4
Keying for permissive schemes	8
Send and receive trip commands	2 to 8

IEEE 1646 specifies performance requirements for a class of protection applications that uses synchronized sampled waveforms, including 87L protection. These requirements are shown in Table II.

Table II
IEEE 1646 Communications Performance Requirements for Synchronized Sampled Waveform Relaying

Data or Application	Time Skew (µs)	Maximum Transfer Time (ms)
Synchronized sampled waveform data for protective relaying	100	<2

IEC TR 61850-90-12, Communication Networks and Systems for Power Utility Automation, provides WAN engineering guidelines for the transfer of the following data types [4]:

- Generic Object-Orientated Substation Event (GOOSE) messages.
- Manufacturing message specification (MMS).
- Sampled Measured Values (SMVs).

Additionally, several latency classes are defined in this technical report; they are summarized in Table III.

Table III
IEC 61850-90-12 Latency Classes for WANs

Class	Latency (ms)	Application
TL5	≤5	87L protection
TL10	≤10	Telecontrol and teleprotection data
TL1000	≤1,000	All other messages

By taking the performance requirements specified in both of these references and including relay manufacturer requirements for asymmetry and restoration, we can establish a summary of the communications channel performance requirements for protection applications. These are shown in Table IV.

Table IV
Communications Channel Performance Requirements for Protection Circuits

Scheme	Latency (ms)	Asymmetry (ms)	Restoration (ms)
87L protection	5	<0.5	5
Pilot protection	8	5	5
Direct transfer trip	10	5	5

IV. Achieving TDM Performance Over Packet-Based Transport

Meeting the performance requirements shown in Table IV is difficult to achieve with a packet-based transport solution because of the packetization of serial data into Ethernet data and the lengthy network-healing algorithms used in Ethernet-based systems [5]. The latency and asymmetry requirements become more difficult to meet if the interface to the relay is a synchronous serial interface such as IEEE C37.94 or Mirrored Bits® communications over EIA-232. The overhead with these interfaces that is associated with packetization and jitter buffering to remove packet delay variation (PDV) leads to increased latency and asymmetry. In this matter, TDM has an inherent advantage over packet-based systems because of its synchronous design combined with its ability to dedicate reserved bandwidth to each circuit [1].

The relative merits of packet-based versus TDM-based systems have been debated for many years. For most industries, the debate is over and Ethernet-based systems have become the clear technology of choice to the extent that there are very few equipment manufacturers still offering TDM-based solutions. The power utility industry is one of the few remaining industries yet to succumb completely to Ethernet because of the predominance of legacy TDM systems, diversity of applications, age of equipment, and need to meet the performance requirements for protection applications that are summarized in Table IV.

The introduction of Carrier Ethernet and MPLS has added a new dimension to the packet-based versus TDM-based system debate for the power utility industry. Fodero and Robertson (2015) explain that:

> Both Carrier Ethernet and MPLS offer improved performance over standard Ethernet by providing advanced quality of service (QoS) schemes and integrated operation, administration, and management (OAM) capability. These improvements enable lower latencies for high-priority traffic and faster network recovery times, bringing network performance closer to that of TDM-based systems. [1]

Despite these improvements, today's teleprotection system migration strategies still force a performance compromise on the end application that results in longer latencies, lack of determinism, and slower healing. One solution to this problem is a deterministic packet transport concept that involves preserving the performance characteristics of TDM with no performance degradation when converting to Ethernet as the transport protocol. The solution simply packetizes a synchronous optical network (SONET) signal and streams it over an Ethernet network. All critical protection data are mapped into a single Ethernet stream and transported deterministically through low-latency tunnels to provide almost the same performance as conventional SONET or synchronous digital hierarchy (SDH) networks (with a unique Ethertype for easy classification). Because the streams are derived from packetized SONET signals, a network using this technology could be considered a "virtual SONET network" or VSN; that is, it would have the same functionality as a SONET network and could have the same performance (except for a negligible increase in latency). Note that the multimillisecond latencies incurred by the conventional pseudowire packetizing of DS0-level signals (voice frequency [VF], IEEE C37.94, etc.) are avoided.

For this solution, there is thus only a single Ethernet stream between each connected substation, with each stream comprising a well-behaved train of regularly-spaced, constant-length packets. For example, to transfer a 51.84 Mbps STS-1 (synchronous transport signal Level 1) VSN stream over a 10 GigE link would require a ~0.1 µs-length packet to be transmitted every ~5 µs. Because such a stream arguably has no significant impact on other network traffic, it can be given access to the network's higher-priority egress queues (discussed in Section VI Subsection C). Assuming the use of "strict-priority" queue schedulers, this guarantees a worst-case PDV for each network egress port (the time for a lower-priority packet to complete an already started egress [e.g., 1.2 µs for a 1,518-byte packet at 10 GigE]). To address the likely concern that a defective VSN source could block other services, particularly network management software (NMS), the VSN ports should have the committed information rates (CIRs) and peak information rates (PIRs) configured appropriately.

This VSN deterministic packet transport approach preserves the ability to maintain native SONET as a transport interface in addition to using deterministic Ethernet as the transport technology, as shown in Fig. 3.

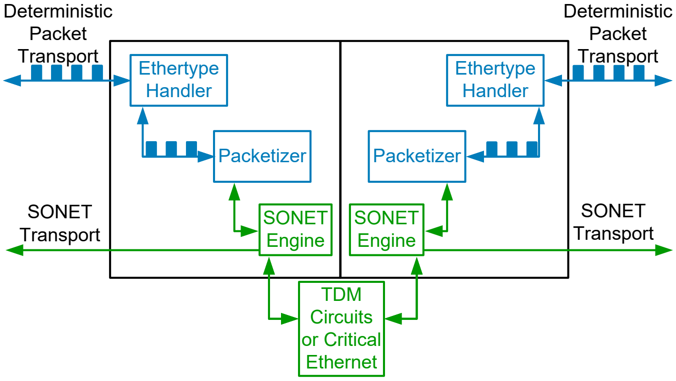

Fig. 3. A hybrid transport network (i.e., VSN) of SONET and Ethernet

V. Power Utility Substation Network Architecture

For the VSN concept to be viable, it needs to support the network architecture models used by the power utility industry. Power utilities run IT and OT services that support a wide range of applications. Utility substations and generation facilities are considered critical assets and contain automation and protection equipment that directly control the operation of the power system. These facilities are networked using a type of WAN that is commonly referred to as an edge network. The utility IT services are typically serviced by a core network that usually requires higher network bandwidths than the edge network does. Fig. 4 illustrates a typical power utility model with both an edge network and a core network.

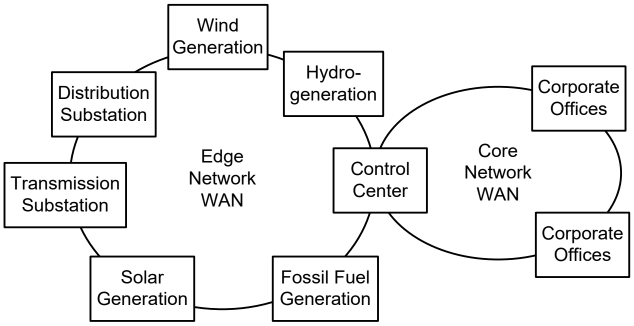

Fig. 4. Power utility edge network and core network model

Because many substation facilities host both IT and OT functions, some utilities integrate core and edge network infrastructures to provide connectivity for services between the substations and the control center as shown in Fig. 5.

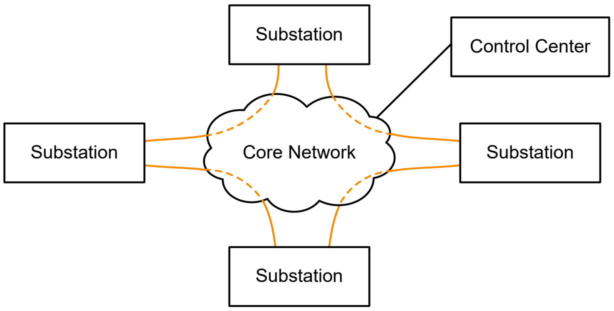

Fig. 5. Integrated edge and core network model

The deterministic Ethernet solution is focused on supporting teleprotection services over Ethernet transport while maintaining the performance currently achieved with TDM-based systems. With the migration of core network technology to packet-based solutions, it is necessary for the VSN concept to support the network topology shown in Fig. 5 where the deterministic Ethernet data are transported from edge network equipment through a core network.

VI. Validation Test Results of VSN Concept

WAN topology and technology are typically selected by an IT department to meet the needs of the corporation. Because the prevailing packet-based transport technologies today are MPLS and Carrier Ethernet, it is important that the OT equipment operating in an edge network (in substations and control facilities) be interoperable regardless of the technology implemented.

The following test results demonstrate that it is possible with the VSN concept to consistently provide low latency, low-channel asymmetry, and extremely fast OT system restoration for failures in the core network regardless of the packet-based transport technology used.

A. Latency Performance Testing and Results

The following test cases provide performance data for SONET encapsulation through an MPLS network and a Carrier Ethernet network. The topology shown in Fig. 6 was used for both of these networks.

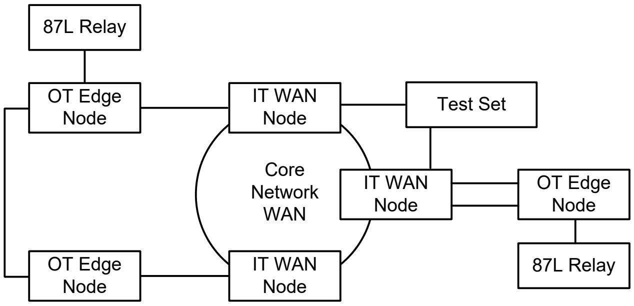

Fig. 6. Test network topology

To establish a set of baseline data, two 87L relays were connected back-to-back with a fiber-optic jumper as shown in Fig. 7.

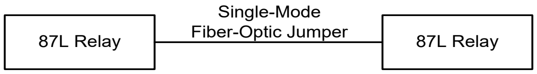

Fig. 7. Baseline data test configuration

Next, the baseline 87L relays were connected to a three-node VSN. The latency and asymmetry information were recorded for comparison against the baseline relay data. Fig. 8 shows the test topology for the VSN test system.

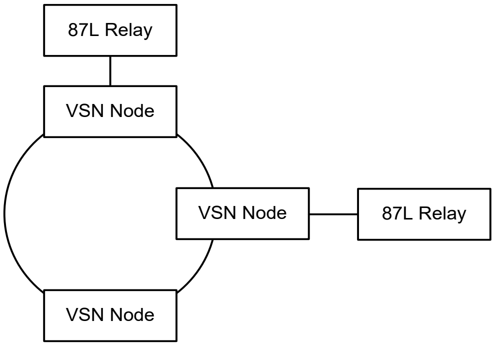

Fig. 8. VSN test network

The VSN test network was then expanded to the topology shown in Fig. 6. A three-node IT WAN was inserted to act as the core network so that the test VSN was tunneled through the WAN and the 87L relays were still connected to the VSN. A test set was used to generate network traffic, simulating typical traffic load conditions. This was done to validate that the core network could use the QoS settings to give the VSN a higher priority over other network traffic in order to maintain deterministic performance.

For the Carrier Ethernet network test, the VSN was given a Fixed Resolved Class of Service (F-RCoS) of 0 and the traffic from the test set was given an F-RCoS of 7. For the MPLS network test, the VSN was assigned a forwarding class of High-1 (H1) and the traffic from the test set was assigned a forwarding class of Expedited (EF).

The testing was performed first over Carrier Ethernet and then again with MPLS equipment inserted in place of the IT WAN nodes shown in Fig. 6. In each test, an 87L relay was used to establish an 87L protection circuit, and the internal measurement capabilities of the relays were used to measure the latency and asymmetry of the channel. The latency and asymmetry performance parameters were recorded for both the Carrier Ethernet and MPLS network implementations. A series of five separate measurements were made in each test, and the average latencies and asymmetries were calculated. The results are shown in Table V and compared with the baseline and VSN-only data.

Each VSN OT edge device used a variable-size jitter buffer based on the PDV of the core network to optimize latency through the IT core network. A PDV setting was used to adjust the size of the jitter buffer. For the Carrier Ethernet network, a PDV of 50 µs was used, and for the MPLS network, 200 µs was used.

TABLE V
COMMUNICATIONS CHANNEL PERFORMANCE TEST RESULTS

Parameter	Baseline (ms)	VSN (ms)	VSN and Carrier Ethernet (ms)	VSN and MPLS (ms)
Latency	0.1	0.1	1.1	1.1
Asymmetry	0.0	0.0	0.04	0.15

The test results in Table V show that the Carrier Ethernet and MPLS core networks in both cases only introduced an additional 1 ms of latency compared with the baseline and VSN-only configurations. The core networks introduced minimal asymmetry, with the Carrier Ethernet network performing better than the MPLS network. In both cases, the results are well within the communications channel performance requirements for 87L protection circuits that are summarized in Table IV. More importantly, the testing validated that appropriate QoS settings can be defined to provide VSN circuits with sufficient priority over other services to ensure the deterministic delivery of VSN frames and thereby preserve the integrity and timing of the encapsulated SONET data.

B. Network Healing Test Results

Network healing performance for the VSN paths can be optimized by provisioning unprotected point-to-point tunnels through the core network. These tunnels are illustrated as dotted lines in Fig. 5 and may also be referred to as “pipes.” Network healing is then performed by the VSN OT edge device rather than by the core network. The following healing tests were performed to measure the comparative performance of edge versus core network failovers. The core network failover test involved breaking the fiber on the link as shown in Fig. 9, and having the core network perform a failover to the redundant path on the opposite side of the ring. In the edge network failover test shown in Fig. 10, a link from the OT edge device to the IT WAN node was broken and healing was performed by the OT edge network.

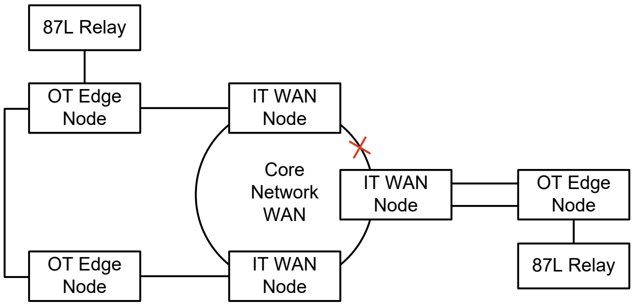

Fig. 9. Core network failover test

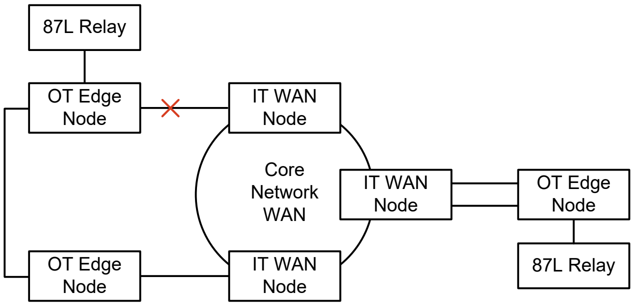

Fig. 10. Edge network failover test

The failover test results in Table VI show that a significant performance advantage can be achieved by using the OT edge network to perform network healing.

TABLE VI
FAILOVER PERFORMANCE TEST RESULTS

Failover Method	Technology	Failover (ms)
Core network	Carrier Ethernet	~50
	MPLS	~50
Edge network	VSN	5

C. Circuit Provisioning and Maintenance

The VSN concept greatly simplifies the provisioning, bandwidth planning, and QoS requirements for operating an OT edge network through an IT core network. The protection VSN requires a minimal CIR throughout the IT core network. The amount of actual bandwidth required is proportional to the number of TDM interfaces required. Typically, this is in the 100 to 250 Mbps range. Because the VSN edge device aggregates all circuits into a single VSN channel, the core network only needs to provision a single service and circuit path with appropriate QoS parameters to tunnel data between OT edge devices.

Network planning is further simplified because only a single QoS value is required for all VSN tunnels across the core network. Within the VSN, all circuits are serviced in real time with minimal jitter. This contrasts with having to manage the QoS for all the protection circuits across the WAN individually. Table VII shows the QoS priority settings that were used for the network healing performance tests.

TABLE VII
CORE NETWORK QOS SETTINGS

Priority Queue	Service
1	Network management
2	VSN
3+	All others

VII. CONCLUSION

A VSN provides a method to deliver mission-critical protection and control system traffic over a packet-based WAN while ensuring that the communications channel performance attributes meet the requirements specified in IEEE 1646 and IEC TR 61850-90-12. A VSN is standard-agnostic and interoperable with packet transport technology (e.g., MPLS and Carrier Ethernet). It elegantly addresses the challenge of migrating TDM-based protection circuits to packet-based transport methods without impacting the performance of the protection application and network. OT network design, planning, and implementation are greatly simplified for complex networks with substation edge and core network elements that involve a combination of manufacturer equipment and transport technology.

This solution uses a simplified provisioning model that easily scales as the network topology changes and grows. Using point-to-point tunnels through the core network with the highest QoS setting below the NMS ensures that the performance of critical circuits are maintained as changes are made on the network, avoiding the need to individually manage each protection circuit. Additionally, even though the traffic has higher priority, the delaying of all the other traffic is negligible (a maximum of 0.1 µs per network link for a 10 GigE core network).

VIII. REFERENCES

[1] 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.

[2] CIGRE Joint Working Group 34/35.11, *Protection Using Telecommunications*, August 2001.

[3] IEEE Standard 1646, Communication Delivery Time Performance Requirements for Electric Power Substation Automation.

[4] IEC TR 61850-90-12, Communication Networks and Systems for Power Utility Automation – Part 90-12: Wide Area Network Engineering Guidelines, 2015.

[5] E. O. Schweitzer, III, D. Whitehead, K. Fodero, and P. Robertson, “Merging SONET and Ethernet Communications for Power System Applications,” proceedings of the 38th Annual Western Protective Relay Conference, Spokane, WA, October 2011.

IX. BIOGRAPHIES

Kenneth Fodero is a research and 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.

Christopher Huntley, P.E., received his M.A.Sc. in engineering physics from the University of British Columbia in 1960. After a two-year Athlone Fellowship in the United Kingdom and a diploma in electrical engineering from Imperial College, Chris joined the research and development group of GTE Lenkurt Electric in Burnaby, B.C. There, he designed both analog and digital (FDM and SONET) multiplexer products, including teleprotection interfaces (DTT, HCB, IEEE C37.94) under a variety of owners from GTE and B.C. Tel through Nortel and GE. In 2007, he started a communications development group for Schweitzer Engineering Laboratories, Inc. in Burnaby, B.C. He is a senior member of IEEE and is active in many IEC, CIGRE, and AES professional groups. He also holds 11 patents on communications circuit technologies.

Paul Robertson is a senior product manager for the wireless networking communications product line at Schweitzer Engineering Laboratories, Inc. (SEL). He has over 25 years of experience developing and marketing products for the telecommunications industry, spanning cellular wireless and wireline communications systems. Paul worked in various technical and marketing roles for Motorola, Hewlett-Packard, and Agilent Technologies before joining SEL. He has a BEng in electrical and electronic engineering from Strathclyde University and an MBA from Edinburgh Business School.

20180209 • TP6813