Ethernet Design for Teleprotection and Automation Requires a Return to First Principles to Improve First Response

David Dolezilek
Schweitzer Engineering Laboratories, Inc.

Presented at the
PAC World Africa Conference
Cape Town, South Africa
July 30–August 2, 2013

Previously presented at
GRIDTECH 2013, April 2013,
and 2012 IEEE Power & Energy Society General Meeting, July 2012

Previously published in
SEL *Journal of Reliable Power*, Volume 3, Number 2, August 2012

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

Ethernet Design for Teleprotection and Automation Requires a Return to First Principles to Improve First Response

David Dolezilek, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Ethernet has emerged as a popular message transport method across many industries, including those considered mission critical, such as electric power, water and wastewater, data centers, and many others. To date, it is most often used for nonmission-critical information technology (IT) messaging, such as supervisory control and data acquisition (SCADA) and configuration access. These data exchanges, characterized as last response, are considered complete based on the delivery of the last message to finish a command sequence. Meanwhile, the mission-critical protection-class operational technology (OT) messages have traditionally been transported over direct serial links. These peer-to-peer data exchanges are characterized as first response because the application requires the delivery of the first message following any fault event. These messages are published after a fault or event malfunction and used in high-speed automation, interlocking, or teleprotection functions. Protection-class digital messaging requires more deterministic message delivery than IT and must meet internationally standardized requirements for message delivery, dependability, and security. Protection, control, and monitoring (PCM) intelligent electronic devices (IEDs) apply IEEE 802.1p and Q parameters to published messages to improve the ability of the network to provide OT behavior. Most IT professionals assume that all perimeter devices, including PCM IEDs, are not capable of managing these parameters and therefore make inappropriate network design choices. In order to transport protection-class messages over Ethernet, IT and OT network engineers must collaborate with protection experts to design the communications to meet OT requirements based on IEC 60834-1, which specifies performance and testing requirements for the teleprotection equipment of power systems. Failure to collaborate on network design has been demonstrated to create unacceptable message delivery delays due to network congestion and rerouting. Each delay is a near miss and has the potential of causing a control system to miss a command to operate. Protection-class messages must travel in a few milliseconds to provoke reaction to a fault or malfunction and cannot survive the same delays allowed for IT networks. If the message is delayed, the message receiver cannot perform mission-critical actions to prevent loss of life, blackouts, or other catastrophes. Power system faults are not frequent; however, the network has to be fast and available every time a fault occurs.**

Peer-to-peer protection-class data exchanges are characterized as first response, which requires the delivery of the first of a burst of messages published after a power system event to complete a high-speed automation, interlocking, or teleprotection function. Today, peer-to-peer communications support many innovative and invaluable applications that require fast and deterministic delivery of every message. Secure and dependable message delivery in first response applications, such as teleprotection, is much more mission critical than client/server applications or other industry machine-to-machine tasks.

Unlike time-deterministic transport methods like synchronous optical network (SONET), which guarantee bandwidth for message delivery, Ethernet is a best-effort technology invented to keep the complexity and cost of a local-area network (LAN) to a reasonable level. Ethernet operates via shared bandwidth methods and therefore with no guarantee of reliable data delivery. Over the last decade, new Ethernet methods and IEEE standards have been created to improve the likelihood that messages are delivered reliably. However, dropped and delayed messages are unavoidable in shared bandwidth networks. In addition, unwanted broadcast messages can cause network congestion, delayed delivery, and unnecessary consumption of processing resources. Regardless of the technology used to transport messages, each delayed or dropped message is a near miss. IT and OT engineers must continue to collaborate using tools, devices, and methods based on IEC and IEEE standards. These networks must be engineered with discipline, not simply assembled.

This paper reviews the first principles of dependable and secure Ethernet message delivery and the methods network designers need to understand and use to increase the likelihood of success.

I. Introduction

The single greatest engineering achievement of the twentieth century was electrification, which forever changed the world and enabled other top engineering achievements.

> Scores of times each day, each one of us taps into vast sources of energy—coal, oil, sweeping winds, rushing waters, power of the atom, and radiance of the Sun itself—all transformed into electricity, the workhorse of the modern world. [1]

Electrification was brought to distant parts of the globe, though not yet all, via vast interconnections of generators, transmission lines, and distribution systems referred to as "the grid." The grid converts various types of energy into dangerous and deadly levels of electricity that is delivered at the speed of light over large distances, converted to safer levels, and consumed as it is delivered because it cannot be stored.

Management of this intricate balance of supply and demand, protection of the delivery apparatus, and preservation of the safety of the public requires the constant, vigilant, sophisticated, and reliable exchange of information among parts of the grid. The addition of distributed and renewable generation, microgrids, two-way power flows, automatic network reconfiguration, and changes in load profiles have required advances in protection and control systems as well. By and large, these advances in real-time information exchange and automatic control within the grid go unnoticed by all but a select few who are aware of high-speed automation, digital teleprotection, and interlocking. High-speed communications among devices performing protection, control, and monitoring (PCM) are largely invisible to the general public—especially if the lights stay on—and even to the utility staff responsible for asynchronous supervisory control and data acquisition (SCADA), energy management, and automation. Unaware that protection-class communications are working in the background of the grid, uninformed people make statements like "the way we generate and distribute electricity today is essentially the same as when Thomas Edison built the first power plant well over 100 years ago." In fact, tens of thousands of PCM intelligent electronic devices (IEDs) are sharing information using information and communications technology (ICT) and making millions of decisions every millisecond of every day to control the health and performance of the grid. Although the underlying principles of generating electricity have not changed, the generators, loads, and digital control systems have changed dramatically. It is the responsibility of all the members of the power industry to maintain and improve service to the public, remain informed of new technologies, and prevent uninformed decisions about grid communications from jeopardizing the delivery of safe, reliable, and economical electric power. Modern PCM digital control systems rely on rapid and deterministic transport of commands via digital messages to avoid potential loss of life, equipment damage, and blackouts by mitigating power system malfunctions and preventing them from creating a catastrophe.

The National Institute of Standards and Technology (NIST) Framework and Roadmap for Smart Grid Interoperability Standards includes IEC 61850 protocols for protection-class communications. The IEC 61850 protocols Generic Object-Oriented Substation Event (GOOSE) and Sampled Value (SV) are Ethernet messages used for peer-to-peer data exchange for automation, interlocking, and teleprotection. SV messages are published at a fixed frequency, often 4,800 messages per second. GOOSE messages are published by IEDs constantly at a configured time between messages. GOOSE messages are also published in a burst mode after a change is detected in the power system. The first message of this burst mode must travel through the network without delay to accomplish mission-critical protection. Guaranteeing undelayed first response of these Ethernet messages requires a revisit to the first principles of network design.

Delayed, dropped, or overcommunicated messages are unavoidable consequences of using Ethernet technology and considered acceptable, even expected, for Internet Protocol (IP) applications. Essentially, this behavior has become the "new normal" because communications designers accept occasional failed message delivery. These delays do not get analyzed as true failures and actual catastrophic near misses. The unintended consequence of the new normal nondeterministic Ethernet is that it is only a matter of time before such a failure occurs, delaying a message burst that is reacting to a change of state in the power system and attempting to perform a protection function.

Near misses are misunderstood, ignored, or, worse, tolerated and accepted because they do not appear to cause immediate or apparent harm. The sole purpose of these communications is to move information instantly after a power system event, and the communications network needs to be designed to that purpose. PCM engineers are obligated to educate end users, consultants, designers, manufacturers, integrators, technicians, and maintenance staff about the expected behavior of communications within protection-class applications. It is imperative to do so because degraded behavior is essentially invisible within the network and others may not grasp the significance of delayed messages. Even when deviations are noticed, network designers, consultants, and integrators often obscure the effect of the symptom, such as by promoting asynchronous rather than synchronous client/server applications, rather than get to root cause.

II. A New Century, a New Challenge

The first decade of the twenty-first century included numerous major grid disturbances. Forensic analysis of these disturbances has indicated that failures in the information communications infrastructure were contributing factors in their development and severity [2]. Additionally, in each case, near misses were observed but not recognized for their importance. Complacency prevented the near misses from being considered true failures and preempted the investigation of the root cause. The initiating events of these disturbances were electrical malfunctions, but the inadequate performance of the information infrastructure disabled preventive actions and caused the malfunctions to escalate into catastrophe. These disturbances serve as a warning to fully understand the acceptance criteria of Ethernet applications and to design for adequate message delivery reliability.

Fundamental errors in providing vital information, inaccurate state estimation, and the lack of alarm signals were contributing factors to the spreading of the disturbance in the North American Northeast blackout on August 14, 2003 [3] [4]. The forensic analysis was hampered by the lack of accurate time distribution to the PCM devices. The Italian blackout on September 28, 2003, was due in part to a lack of proper communication and cooperation between the Swiss and Italian operators, which led to delayed corrective actions, resulting in the disconnection of the load of the whole peninsula [5] [6]. An inaccurate interpretation of an alarm signal was one of the key events in the evolution of the London blackout on August 28, 2003 [7].

Though the definitive root cause has yet to be determined, numerous investigations indicate that the failure of the information and control system for Turbine 2 was part of the cause of the Sayano-Shushenskaya hydroelectric power station failure. Listed among the numerous contributing factors is the failure of the ICT system to effectively signal a vibration alarm. A chain reaction, including an incorrectly operating control system followed by the failure of the safety system, turned a malfunction into a catastrophe that resulted in the death of 75 people.

In addition to control system failures with substations and distribution networks, examples of failed information systems are numerous within industrial control systems as well. Loss of life due to arc flash is statistically a daily occurrence in the United States [8]. Instantaneous communication of the presence of light from an arc, in conjunction with measurement of energy feeding the arc, facilitates quicker detection and mitigation. Whether transmitting light or a message conveying the presence of light, each millisecond of delay allows the fault to grow in strength and thus increases damage or injury.

Perhaps the most notorious example is the 2010 tragedy on the Deepwater Horizon oil platform in the Gulf of Mexico that was impacted by a failed alarming and control system and led to the death of 11 people [8].

Each of these examples points to the need to understand and meet the needs of each application as well as heed near miss observations. Of course, failure of any device, apparatus, or communications link may cause a system failure. This paper focuses on appropriate design to pursue communications network excellence. When shared bandwidth Ethernet is used to build modern ICT networks, designers must be aware of the acceptance criteria of all classes of communication.

III. New Challenges Require Revisiting First Principles

A. Indefinite Ethernet Message Behavior Prohibits Innovative Improvements

The operation times of circuit breakers and other primary equipment cannot be shortened and, in fact, may slow because physical attributes affect components in service. Therefore, in order to improve the performance of teleprotection and telecontrol, ICT systems must reduce the transit time of messages. As interconnections and distributed generation make the power system more sophisticated, it is essential that we also increase the dependability and security of communications [9].

The ability of microprocessor-based PCM IEDs to compute, remember, and communicate (considered smart behavior or a smart grid) ushered in a wave of modernization starting in 1984. Digital communications with PCM IEDs began with the introduction of microprocessor-based devices with command line interface (CLI) capabilities. Interacting with the CLI, a person or a program acts as a client of data being served from the IED. PCM IEDs began detecting faults and tripping circuit breakers, as well as sharing information via digital communications.

Protection-class data exchanges began in 1994 when peer-to-peer communication was introduced into IEDs via Mirrored Bits® communications. Mirrored Bits communications, EtherCAT, and IEC 61850 GOOSE messages used in protection-class applications today are characterized as first response because the application requires delivery of the first message following any fault event. These messages, which are published periodically (as well as immediately) after a fault or event malfunction, are constantly operating in the grid to maintain the safety and stability of global power systems.

Many designers and end users do not notice or are willing to accept the latency, jitter, nondeterminism, and dropped packet behavior of Ethernet networks. The danger in this is threefold:

- Lower quality of service becomes normal.
- Future innovations to real-time synchronous client/server applications and closed-loop automation will not be possible or will have diminished capacity due to lower quality of service.
- Peer-to-peer telecontrol and teleprotection applications cannot be implemented on these networks or will have diminished capacity due to lower quality of service.

Over the past decade, power system operations, similar to many other industries, have knowingly lowered the bar for an acceptable class of service for client/server communications as new technologies have been deployed (the new normal). To an alarming degree, this is happening to operators of mission-critical services, such as power systems, as public communications infrastructures are modernized with information technology (IT) methods, such as IP and multiprotocol label switching (MPLS), to improve revenue by sharing bandwidth among multiple users. IT designers often describe their systems as deterministic because dropped packets are resent and delayed packets are buffered and resent. However, these are recovery mechanisms for the failure to provide actual deterministic behavior. Operational technology (OT) networks, especially those required to prevent potential loss of life, require true deterministic delivery of every packet, every time, on time.

In the past, IT applications benefited from sharing the deterministic communications previously installed for OT applications and perhaps enjoyed a higher quality of service than absolutely necessary.

Because convenient Ethernet IT satisfies legacy client/server OT requirements, it is often used without consideration of improved client/server performance or wide-area peer-to-peer applications. Once in place, poorly designed Ethernet and IP ICT systems prohibit innovation, such as synchronous SCADA and stability controls, including real-time synchrophasors and wide-area IEC 61850 GOOSE.

B. Indefinite Ethernet Message Behavior Is Incorrectly Interpreted as Resilience

An Ethernet network commonly includes Ethernet and IP methods that use data-packet-based technologies because of convenience, flexibility, and multipurpose networking. Each message becomes a packet that is funneled into a multipurpose network. The network queues up and then delivers messages on a first come, first served basis. If the Ethernet switches understand the specialized message prioritization, these messages will go to the front of the queue. This process is repeated for each switch that the message passes through. Packet-based networks, like Ethernet, share the available communications bandwidth (or nondefinitive provision capacity) in an ad hoc manner. Thus nonspecific amounts of time are provided to various applications as needed, and the traffic fluctuates.

When the volume of traffic increases, the message latency may increase. When the network changes to reroute traffic, the message latency may increase. If a high volume of multiuse traffic causes a switch to drop a packet, the message latency definitely increases or the message may never be delivered. This indeterminate behavior of Ethernet is characterized as a cloud because it is not clear which path a message will take; it is impossible to predict behavior with certainty; the message delivery forecast is cloudy. This indeterminate behavior is also an indication of near misses, each of which identifies when teleprotection messages may be delayed.

We must understand the first principles of Ethernet to adequately constrain its shared bandwidth behavior for delivery of protection-class messages.

IV. Ethernet First Principles Have Evolved

In 1983, the IEEE standards board approved the first IEEE 802.3 Ethernet standard. Over time, Ethernet and IP methods were developed in various industries to make it convenient to route message packets indirectly to a communications network address rather than a dedicated device address. Logical and physical message paths rarely match because messages travel indirectly to their destination via many network routing, queuing, prioritization, and network reconfiguration technologies. The simplicity of Ethernet network devices providing message routing with no pre-engineering creates the convenience that was previously mentioned. However, Ethernet is described as a best-effort ICT due to inevitable and unavoidable dropped packets that result from routing, redirection, queuing, and bandwidth saturation. Inevitable packet loss remains the largest difference between an indirect Ethernet cloud and a direct serial cable.

Therefore, many modifications have been required in an attempt to overcome dropped packets that result from routing, redirection, queuing, and bandwidth saturation. For network devices, these modifications include:

- Replacement of IEEE 802.3 collision domains with ISO/IEC 15802-1 media access control (MAC) address services and addition of IEEE Ethertypes for power system peer-to-peer messaging.
- Adoption of IEEE 802.1p message packet prioritization and IEEE 802.1Q message segregation into virtual local-area networks (VLANs).
- Use of Rapid Spanning Tree Protocol (RSTP) to help to reconfigure broken network segments within minutes. It restores service to peripheral IEDs within tens of minutes. Proprietary network reconfiguration methods faster than RSTP have been developed by each Ethernet switch manufacturer. These private methods can reconfigure broken network segments within seconds and provide service to IEDs within tens of seconds.
- Investigation of industrial process redundancy protocols to compensate for dropped packets via duplicate networks using Parallel Redundancy Protocol (PRP) or High-Availability Seamless Redundancy (HSR) protocol, along with consideration of the addition of an HSR or PRP Redundancy Box (RedBox) at each IED and client location to support duplicate network connections to a single device network address.
- Expanse of duplicate Ethernet networks to increase the likelihood that both do not drop the same packets.
- Use of MPLS for wide-area network (WAN) connections, which works by tagging the traffic, such as Ethernet packets, with an additional identifying label to distinguish the label switched path (LSP) the packet will take. A simplistic view is that this works similar to IEEE 802.1Q tags within a local-area network (LAN).

In summary, dropped packets are inevitable in Ethernet networks. Rather than getting to root cause, the industry has pushed correction mechanisms to the users of the network, the peripheral IEDs. IEDs must now assign IEEE 802.1p message priority. Anytime a technology resorts to prioritization, it is admitting that it cannot meet the specification 100 percent of the time. Priority allows the Ethernet network to transport some messages ahead of others, but not guarantee delivery security or dependability. Failure and reconfiguration cause buffering and retransmission of unwanted messages in lieu of redundant Ethernet paths. HSR and PRP create an unwanted message in conjunction with each wanted message in an effort to mitigate inevitable message loss. All of these unwanted messages act to reduce the dependability of the application.

V. IT Addresses Near Miss Symptoms While OT Would Prefer to Correct Root Cause

A. Ethernet Failure and Recovery Method Less Dependable Than Redundant Connections

OT mission-critical applications often demand redundant devices and communications. Though Ethernet technology physically appears to provide multiple data paths in the cloud, it actually denies the ability to have redundant message paths active simultaneously. Instead, the network will react to a failed connection with path information messages exchanged among switches and then reconfiguration to create a new route.

B. New Route After Ethernet Reconfiguration May Have Different Path Performance

OT operators prefer to know the path that messages are traveling. Dynamic reconfiguration after a failure creates new message routes that may behave differently and may not be visible to the operator but remain in the cloud. This also makes troubleshooting and diagnostics difficult.

C. Ethernet Failure and Recovery Method Adds Complexity to the Peripheral Devices

Ethernet congestion or reconfiguration causes buffering and resending packets after failure. This transfers the burden to the peripheral devices to manage lost and repeated messages.

D. Ethernet Traffic Routing Techniques to Mitigate Congestion Add Complexity to the Peripheral Devices

PCM IEDs have evolved to include additional processing and memory to manage IEEE 802.1 QVLANs and other message navigation methods on multicast messages and not on IP messages. This added burden on the peripheral device provides message header information for use by the Ethernet network devices to segregate and prioritize multicast messages.

E. Ethernet Traffic Routing Techniques Within Peripheral Devices Confuse IT Experts and Technology

IT technology treats ports as either a "trunk," connected to another Ethernet network controller, or an "edge," connected to a device with an Ethernet port but no network control capabilities. Now that PCM IEDs must manage IEEE 802.1 QVLANs, they require neither a trunk nor an edge connection. They require a new category for a peripheral device with some network control, such as VLAN management, but not all the features expected for a trunk.

F. Inevitable Dropped Packets in Ethernet Networks Add Complexity to the Peripheral Devices

Redundancy protocols, in lieu of unavailable redundant paths within Ethernet, again move burden to the peripheral devices. PCM IEDs will need to transmit and receive two messages for each data transfer to improve the likelihood that one of the messages will make it through the network.

G. Internet and IP Quality of Service (QoS) and Low Latency Queuing Do Not Guarantee Better Service Quality

Ethernet network devices use QVLAN priority, IP QoS, and low latency queuing to transport a class of messages with better precision than other messages. This is actually an improved class of service where these messages are queued ahead of other messages, but still no guarantee of speed or delivery is made when a queue becomes saturated.

VI. New Challenge, Same Requirements

Security of communications-assisted protection and control requires deterministic latency of each message delivery. For example, security of a mission-critical control means to refrain from tripping a breaker when not required to trip. A secure OT network is designed to guarantee deterministic, on-time delivery of each blocking or interlocking message. OT security means every message is delivered with predetermined maximum latency. IT networks are instead designed to buffer and redirect traffic to increase the likelihood that the message will eventually be delivered. Message propagation delays of IT networks may cause protection and control problems.

Dependability of communications-assisted protection and control requires delivery of each message. For example, dependability of a mission-critical control means to perform tripping when a breaker is required to trip. A dependable OT network is designed to guarantee deterministic, on-time delivery of each tripping or control message once and only once. OT network dependability means reducing lost messages to near zero. A dependable IT network is instead designed to send and resend messages to increase the likelihood that one message eventually makes it through. IT dependability means the network detects and resends lost messages. However, resent buffered messages of IT networks may cause protection and control problems.

As protection-class communications are deployed in new mission-critical applications and new ICT networks, it is crucial to understand that performance must not degrade to create near misses. Dependability and security to deliver every message uncorrupted every time are specifically essential for telecontrol, teleprotection, interlocking, and high-speed automation. IT, OT, protection, automation, and communications engineers must collaborate and acquaint themselves with IEC 60834-1 [10]. This standard defines message delivery security and dependability requirements that Ethernet networks must satisfy if they are to be used for digital high-speed automation, interlocking, and teleprotection.

Because Mirrored Bits communications and EtherCAT traverse separate private direct links, there is no opportunity for congestion or reconfiguration that will result in dropped packets or unexpected devices or network configuration that results in extra messaging. They intentionally do not multiplex other communications in order to maximize the speed, dependability, and security of message delivery.

As mentioned, it is impossible to create Ethernet networks with 100 percent dependability and security. Also, substandard performance is not easily detected, so when used in mission-critical applications, it is especially important that the degradation be identified, measured, and improved. ICT designers must acknowledge the responsibility for reliable message delivery. They must use every tool and method available to remove as much risk of dropped packets and potential catastrophic failure as possible.

If the network is designed to satisfy protection-class communications, the other messaging on a shared bandwidth network will also enjoy greater security and dependability. This better message performance will encourage innovation and improvements in these other applications as well.

Both noise and, in the case of a shared Ethernet network, delivery of unwanted and low-priority messages adversely affect the delivery of appropriate protection-class command messages. Unneeded and unwanted messages have the possible impact of being interpreted as a legitimate command, reducing security, or consuming processing resources in the network or PCM device and causing incorrect processing of a legitimate command message, reducing dependability.

The National Electrical Code (NEC) is the most complete set of electrical code requirements that govern electrical wiring installations in the interest of safety for people and property. The NEC provides examples for installing conduit and cable trays to improve the performance and longevity of ICT cables in service. These examples illustrate the increased possibility of interference at splices and interconnections, regardless of cable type. Switched and spliced Ethernet will be more susceptible to noise than long runs of serial or Ethernet cables.

OT security is the ability to prevent interference from generating a command state at the receiver when no legitimate command was sent. Subscription to Ethernet multicast is not source specific, so multiple PCM IEDs can intentionally or accidentally publish GOOSE commands with identical message attributes. Therefore, application security is the ability to appropriately not accept as a command an incorrectly received message either corrupted in transit or received from an incorrect source. A practical approach to determine security was made by the IEEE PSRC Working Group I3 [11]. The working group suggests measuring security as the number of false trips, or protection system near misses, relative to the total number of events recorded during a time period. For a communications-assisted application, this equates to the number of incorrect messages, interpreted as legitimate commands, received and acted on by a device relative to the total correct command messages recorded during a time period. It is not possible to know the application impact from an Ethernet communications perspective; therefore, the network security measure is simply the number of incorrect, unwanted, and unneeded messages delivered over time relative to the total number of wanted messages. IEC 60834-1 Section 4.3.2.1.1 is the appropriate reference to illustrate the required application resiliency to communications channel noise and congestion. It describes the probability of an unwanted command P_{uc} to be approximated as follows:

$$P_{uc} \approx \frac{N_{uc}}{N_B} \tag{1}$$

where:

N_{uc} is the number of unwanted commands recorded.

N_B is the number of error bursts or unwanted messages.

The application security is then given by $1 - P_{uc}$.

The probability of a device receiving an unwanted message P_{um}, regardless of how it deals with it, is approximated as follows:

$$P_{um} = \frac{N_{umr}}{N_{umt}} \tag{2}$$

where:

N_{umr} is the number of unwanted messages received by the device.

N_{umt} is the number of unwanted messages transmitted into the network.

The communications channel security is then given by $1 - P_{um}$.

Communications channels may also disturb a communications-assisted application by delaying the arrival and processing of a command at the receiving device. OT dependability is the ability to cause a valid command action via a digital message in the presence of interference. Therefore, IEC 60834-1 Section 4.3.2.2, which discusses dependability, is another appropriate reference. It describes the probability of missing, or not receiving, a command P_{mc} for a fixed actual transmission time, to be approximated as follows:

$$P_{mc} \approx \frac{N_T - N_R}{N_T} \tag{3}$$

where:

N_T is the number of commands sent.

N_R is the number of commands received.

The application dependability is then given by $1 - P_{mc}$.

The probability of a device missing a message P_{mm} for a fixed actual transmission time is approximated as follows:

$$P_{mm} = \frac{(N_{tm} - N_{wmr})}{N_{tm}} \tag{4}$$

where:

N_{tm} is the total number of wanted and unwanted messages transmitted.

N_{wmr} is the number of wanted messages received.

The communications channel dependability is then given by $1 - P_{mm}$.

Though not exhaustive, Table I provides the required security and dependability for digital messaging within several protection schemes. These requirements must be understood and satisfied by Ethernet network designers planning to use Ethernet connections among PCM IEDs for local- and wide-area high-speed automation, interlocking, and teleprotection.

TABLE I
PERFORMANCE GUIDANCE FIGURES FOR VARIOUS TELEPROTECTION SCHEMES

Protection Scheme	Security P_{uc}	Dependability P_{mc}
Blocking	$<10^{-4}$	$<10^{-3}$
Permissive Underreach	$<10^{-7}$	$<10^{-2}$
Permissive Overreach	$<10^{-7}$	$<10^{-3}$
Intertripping	$<10^{-8}$	$<10^{-4}$

For an Ethernet network, a commissioning test needs to be designed to provide the following measures:

- Application security based on the number of unwanted Ethernet message commands acted on by a PCM IED relative to the number of unwanted Ethernet message commands sent to that PCM IED.
- Communications channel security based on the number of unwanted Ethernet messages received by a PCM IED relative to the number of unwanted Ethernet messages sent to that PCM IED.
- Application dependability based on the number of legitimate Ethernet message commands received by a PCM IED relative to the number of legitimate Ethernet message commands sent to that PCM IED.
- Communications channel dependability based on the total quantity of Ethernet messages received by a PCM IED relative to the number of legitimate Ethernet messages received by a PCM IED.

Private direct dedicated channels for teleprotection, interlocking, and high-speed automation make observing message behavior quite simple. Many PCM IEDs internally calculate and trend these measures. The shared bandwidth behavior of Ethernet makes it very difficult to measure these four performance criteria. Further, IT applications do not require these criteria, so tools to observe and measure them do not exist. However, some PCM IEDs do monitor the multicast message parameters sequence number and state number in order to detect when a wanted message was not received.

Any additional messages in the network will directly affect dependability measures. Newly added IEDs, poor network configuration, and malfunctioning IEDs can each produce unwanted messages that reduce dependability.

As an example, consider an application supported by a GOOSE exchange between two PCM IEDs. A typical GOOSE repetition rate of once per second, when ignoring burst mode, requires the exchange of 86,400 messages a day. Aggressive burst mode will improve application performance but is momentary, occurs only during a detected event, and contributes less than ten messages to the total. Table II illustrates the number of wanted GOOSE messages in this single exchange that may be delayed while meeting the security criteria. Table II also illustrates the number of unwanted messages allowed to be delivered in order to meet the dependability requirement.

TABLE II
PERFORMANCE GUIDANCE FIGURES FOR SINGLE GOOSE EXCHANGE WITH 1-SECOND DELAY BETWEEN PUBLICATIONS

Protection Scheme Via 1-Second GOOSE Repetition	Security P_{uc}	Dependability P_{mc}
Blocking	<9	<86
Permissive Underreach	<1	<864
Permissive Overreach	<1	<86
Intertripping	<1	<9

Now consider a network where a single unwanted GOOSE exchange is allowed to reach the receiver. This is typical when configurations do not correctly filter unwanted messages based on a VLAN or MAC address. This will result in 86,400 unwanted messages per day, which alone makes communications for an intertripping scheme 500 times less dependable than required.

Compensation techniques to improve security against inevitable dropped packets within Ethernet ICT networks often have an adverse effect on the peripheral devices. Redundant messaging performed by the IED, such as PRP, which requires duplicate publications of each message, does increase the security of the Ethernet network, but at the cost of making an intertripping scheme 500 times less dependable than required. In addition, it forces the PCM IED to process twice as many publications and subscriptions rather than have the network devices eliminate the root cause.

VII. FOR THE NEW SOLUTION, A MODERN METHOD

Electric power improves lives, but control of that power comes with great responsibility. After a decade of carefully designing teleprotection over Ethernet and working to create international standards and best engineering practices, it is our obligation to share what we know. Explaining the potential danger of Ethernet near misses should raise awareness, create a healthy foreboding, and lower our complacency.

If applied incorrectly, modernization to replace repetitive simple processes, like installing and terminating copper wires among field devices and IEDs, may accidentally introduce new solutions that harbor unintended complexity, like Ethernet traffic engineering. It is essential to not choose Ethernet simply as a method to replace the labor of craftsmen installing hard-wired point-to-point connections with an Ethernet connection to a network cloud. Applying Ethernet without appropriate network engineering bypasses the human element of thinking, problem solving, and designing for reliability. It is necessary to use new ICT tools to modernize best wiring practices and convert them to best practices for virtual connections over Ethernet. The added complexity to the network configuration for traffic engineering is necessary to provide OT protection-class communications. Ethernet networks must be engineered, not simply assembled.

Best engineering practices to reduce the number of near misses in the delivery of messages on shared bandwidth Ethernet networks are based on international IEC and IEEE standards. PCM IEDs are expected to use Layer 2 multicast messages and follow these rules for adding network engineering parameters:

- Assign each GOOSE message a unique VLAN based on IEEE 802.1Q, referred to as a QVLAN.
- Assign each GOOSE message a unique IEC 15802-1 multicast MAC address.
- Assign each GOOSE message a unique application identifier (app ID).
- Assign a descriptive GOOSE identifier (GOOSE ID) rather than generic IDs in the IED to improve documentation and troubleshooting.
- Label GOOSE message payload contents with descriptive names, rather than generic names, in the IED to improve documentation and troubleshooting.
- Carefully design payload size and contents to facilitate appropriate GOOSE application processing—*mind the gap*.
- Carefully choose IEDs that process incoming GOOSE messages appropriately fast for protection-class applications— *mind the gap*.
- Do not publish multicast messages on the network without QVLAN tags.
- Disable all unused PCM communications ports.
- Monitor GOOSE message attributes to derive the quality of the message.
- Use the GOOSE attributes of sequence number and state number to determine if all wanted messages reach the receiver.
- Monitor, record, and alarm failed quality of GOOSE messages.
- Provide GOOSE reports with configuration, status information, and statistics pertaining to GOOSE messages being published and subscribed to by the IED.
- Record and alarm failed quality of GOOSE messages for use in local and remote applications.
- Display status of GOOSE subscriptions and alert operators of failure.
- Configure each switch port to block the ingress of unwanted and allow wanted multicast messages via VLAN and MAC filtering. This reduces the multicast traffic through the network to only that which is required.
- Configure each switch port to block the egress of unwanted and allow wanted multicast messages via VLAN and MAC filtering. This prevents unwanted messages from reaching the IEDs.
- Use switches designed for rugged environments and Layer 2 multicast among PCM IEDs in a fixed address network.
- Do not allow dynamic reconfiguration; this leads to unknown network configurations.
- Use switches that provide real-time status of traffic behavior and network configuration.

It is very important to note that though the established and standardized practices for engineering message delivery through an Ethernet network add complexity, they are both necessary and nearly impossible to add to an in-service network later.

Do not assume that the adoption of Ethernet eliminates the requirement to think about the virtual wires within the cloud. Physical craftsmanship is replaced by sophisticated network engineering. Even though it is not possible to verify dependability and security over a shared bandwidth network, these internationally standardized best practices have been developed to maximize the likelihood of success.

VIII. It Is Everyone's Job to Understand, Identify, and Mitigate Risk

Over the past decade, power system operations, similar to many other industries, have knowingly and unknowingly weakened the acceptance criteria for client/server communications as new technologies were deployed. This change mirrors the adoption of personal mobile telephones over fixed landline service. The performance of mobile services is much less reliable than landlines, with dropped calls and noisy connections, but the convenience of mobility makes the degraded service acceptable to most users. In fact, many people find that they do not need the quality of service of a personal landline telephone, terminate the service, and maintain only a mobile telephone. To an alarming degree, this is happening to operators of mission-critical services, like power systems, as public communications infrastructures are modernized with IT methods, like IP and MPLS, to improve revenue by sharing bandwidth among multiple users.

The IEEE 1613 standard details environmental and testing requirements for communications networking devices in electric power substations. IEEE 1613 and IEC 61850 Part 3 have influenced manufacturers to increase the reliability of Ethernet switches to be similar to the modems and port switches they replace as they move from the office environment to the field. OT applications require that Ethernet switch reliability increases to match that of the PCM IEDs because they replace wiring and cabling directly between IEDs for protective interlocking.

A. The New Crisis

The degraded performance of communications based on the new shared bandwidth techniques of Ethernet and MPLS often goes unnoticed or, worse, noticed but not alarmed. A more convenient but lower class of service for personal and business communications has led many people to accept dropped calls and late email delivery and ignore them as near misses. Consider that had these failures been part of a mission-critical data exchange, the results may have indeed been catastrophic. As described in "How to Avoid Catastrophe" in *Harvard Business Review*, near misses are among the often unremarked small failures that permeate day-to-day business but cause no immediate harm. People are prone to misinterpret or ignore the warnings embedded in these failures, so they often go unexamined or, perversely, are seen as signs that systems are resilient and things are going well [12].

B. Casual Common Ethernet Methods Are Not Acceptable for PCM

The secure and dependable use of Ethernet between devices on a LAN, such as between relays, requires a solid understanding and application of first principles, including payload, packet, and addressing at the data link layer, Layer 2 of the seven-layer Open Systems Interconnection (OSI) model for protocols. The seven layers of the OSI model include: physical (Layer 1), data link (Layer 2), network (Layer 3), transport (Layer 4), session (Layer 5), presentation (Layer 6), and application (Layer 7). IP methods use a four-layer Internet model and focus on addressing at the network layer to communicate between networks, such as between a SCADA computer and a remote relay or remote terminal unit (RTU). The four layers of the Internet model include: link (Layer 1), Internet (Layer 2), transport (Layer 3), and application (Layer 4). This Internet model is simpler and allows shortcuts for casual configuration, but does not support the multicast messages at Layer 2 of the OSI model. This difference requires a return to the first principles of Ethernet underlying both stacks and an understanding of, and adherence to, the best engineering practices listed earlier. IT and OT subject matter experts must collaborate with protection engineers to correctly apply protection-class communications over Ethernet.

It is important to note that the same Ethernet ports that support IP traffic in the PCM IEDs also provide mission-critical peer-to-peer protection-class messaging. Therefore, these peer-to-peer Layer 2 GOOSE and SV multicast messages often must share the same Ethernet network as the client/server IP traffic. This single port, often designed with physical redundancy, blurs the differences between Layer 2 and Layer 3 message behavior and requirements. IP methods in the relays also shortcut and ignore the data link layer of Ethernet communications. This shortcut is the root cause of misunderstanding among ICT designers about the impact of casual Ethernet design on critical communications.

Automatic IP addressing and Ethernet message routing are convenient for large and constantly changing networks of devices that frequently are replaced or moved. They are also convenient to send messages to every node in the network, which is why Internet spam is so easy, promiscuous, and successful. However, neither of these scenarios is desirable within PCM networks—in-service network devices rarely change location or address and messages need to travel to a select few destinations rather than all nodes. Also, out of the scope of this paper but still important, Ethernet and IP methods and routable messages introduce additional cybersecurity concerns.

Ethernet for ICT must be done with products designed for the task and thoughtful specification, design, construction, and testing of Ethernet networks to support the underlying critical OT that protects people and apparatus and preserves grid stability.

Near misses need to be driven to root cause rather than create a new normal. Ignoring near misses contributed to the disaster that befell the *Columbia* space shuttle in 2003. One wing of the shuttle was damaged by insulation foam falling from the external fuel tank during liftoff, causing the shuttle to break apart as it reentered the atmosphere [12]. The foam issue was known to managers since the start of the shuttle program. They were concerned early on, but because there were no serious mishaps in the first dozen flights, the managers began to consider the foam strikes as maintenance issues instead of near misses. As with the concept of the new normal of degraded performance of digital messages in an Ethernet network, the foam strikes became a case of normalization of deviation from specification: the new normal. Even after a dramatic foam near miss that was under investigation, the *Columbia* was launched as planned in part due to desensitization to the deviations and also political and social pressures to support the International Space Station. According to the Columbia Accident Investigation Board, "the pressure of maintaining the flight schedule created a management atmosphere that increasingly accepted less-than-specification performance of various components and systems" [12].

Power system application designers and testers are under pressure to design and commission digital communications systems with complicated Ethernet technology that was originally intended for other purposes. The apparent success of poorly designed in-service substation Ethernet systems, where near miss delayed messages have not yet overlapped a message burst during a power system failure, may also encourage designers to take shortcuts. Therefore, automation and Ethernet experts, unaware that they should be coordinating with mission-critical application experts, accidentally provide advice without a full appreciation for interlocking and teleprotection communications requirements and influence the bias of the designers toward using IT design practices rather than OT. A good question for an end user to ask would be, "If I had more time and resources to learn, understand, and test, would I make the same design decision?"

IX. Evolution of PCM IT and OT

The single largest communications technology challenge facing the power system industry today is the inappropriate use of IT in OT networks. Ethernet is essentially synonymous with IT in many industries and is chosen without regard for support of the underlying applications and, in some cases, contrary to the needs of those applications. This is further complicated by the fact that the power industry, like others, has migrated toward the use of a single Ethernet connection on computers and IEDs to support numerous simultaneous IT and OT conversations.

As previously mentioned, PCM IT began when ICTs moved into the grid as electromechanical devices (which are based on the physics of electromagnetism causing metal platters to spin) were replaced with smart devices with onboard computing for conversion of analog signals to digital measurements, memory, and communications. Since 1984, digital communications with PCM IEDs have allowed people or programs to act as a client of data being served from the IED. People began sending and extracting settings and retrieving disturbance records (similar to oscilloscope captures stored during a power system event) and reports that gave a calculated distance to the fault and information about the health and behavior of power system apparatus. Soon after, PCM IEDs were enhanced to support operator client/server OT communications, via an operator console, to exchange information with PCM IEDs to perform remote control.

These OT client/server applications were designed to survive the asynchronous nature of historically poorly performing client/server request-and-response data acquisition communications mediums and protocols, including the following:

- Variable message response and delivery latency and asynchronous server data due to the lack of time synchronization of the IEDs.
- Occasional loss or corruption of messages.
- Incoherent data due to the lack of orderly continuity, organization, and perhaps relevance—information simultaneously presented to the client is actually created and collected from the servers at very different times. A Boolean change of state updates more quickly than analog voltage and current measurements.
- Incoherent wide-area data due to locations responding at different times—locations update in a round-robin poll-and-response scheme, so some data are recent while others are at least as old as the time duration of the polling sequence, which is often several minutes.

Operators today still experience infrequent and unsynchronized updates from field devices. Users have been trained to overlook incoherent information that results from asymmetric acquisition of analog versus digital data and from near and far source locations. These data exchanges, characterized as last response, are completed with the delivery of the last message to finish a command sequence. During this continual asynchronous data acquisition, the control system is constantly attempting to represent the present state of the power system. However, this representation is never the actual state of the power system, but rather it is the present state of the last response data acquired about the power system.

As mentioned, the appearance of MIRRORED BITS communications in 1994 again modernized the grid with data exchange directly between smart devices in the grid. This results in better, faster, and automatic decision making. First response applications require the delivery of the first of a burst of messages that are published after a power system event to share information as quickly as possible. Finally, decades after the first smart relay, smart meters were deployed to replace their electromechanical counterparts. Most residential meters in service today are based on the physics of electromagnetism causing metal platters to spin and are slowly being replaced with smart devices that compute, remember, and communicate. Twenty-five years after it began, the migration of ICT into the grid reached the consumer. No longer invisible, intelligent devices with computing, memory, and communications can be seen by the general public on the periphery of the smart grid.

When using Ethernet, where the cables go, how many peer-to-peer connections are added to the system, what other communications are added, and what happens to the power system all directly impact both IT and OT applications. Peer-to-peer connections in these Ethernet networks are not physically isolated but rather are being distributed among all the other message traffic within the Ethernet cloud and must carefully be virtually isolated.

PCM OT networks are often local networks that support a substation and may also cover their neighboring distribution circuits or WANs connecting several substations. For example, Fig. 1 shows several local OT networks communicating mission-critical information over wide-area OT networks. This information, including teleprotection signals, synchrophasors, SCADA data, system integrity protection scheme (SIPS) arming data, SIPS contingency alarms, and SIPS mitigation control, is traditionally transported via OT network methods. Wide-area OT methods, such as time-division multiplexing (TDM), provide the deterministic and high-availability characteristics necessary for mission-critical electric power system applications.

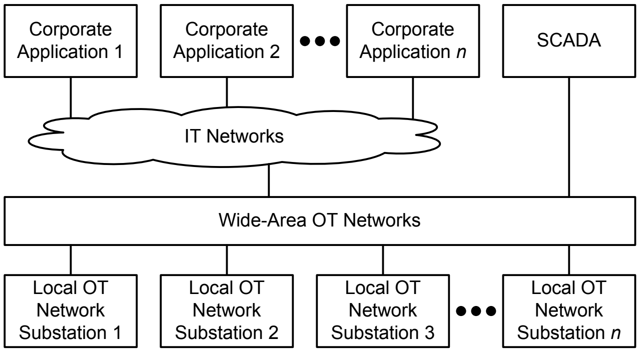
Corporate Application 1
Corporate Application 2
Corporate Application *n*
SCADA
IT Networks
Wide-Area OT Networks
Local OT Network Substation 1
Local OT Network Substation 2
Local OT Network Substation 3
Local OT Network Substation *n*

Fig. 1. Local OT Networks Communicate Mission-Critical Information Over Wide-Area OT Networks

If a single but unwittingly insufficient IP method is promoted for all grid communications, it will be able to support IT information and some, but not all, client/server OT applications with their present performance criteria, with no room for innovation or support of protection-class OT. In this case, the crucial, mission-critical protection and control actions in service today that need to be further deployed to modernize the grid require a separate and deterministic network with near-zero message loss. Of course, the best solution is to use forethought to deploy a single ICT communications infrastructure that supports mission-critical actions, as well as delivery of other information, such as metering. Fig. 2 illustrates that even if IT networks are installed to move nonmission-critical business information, a separate wide-area OT network is still necessary for mission-critical PCM applications.

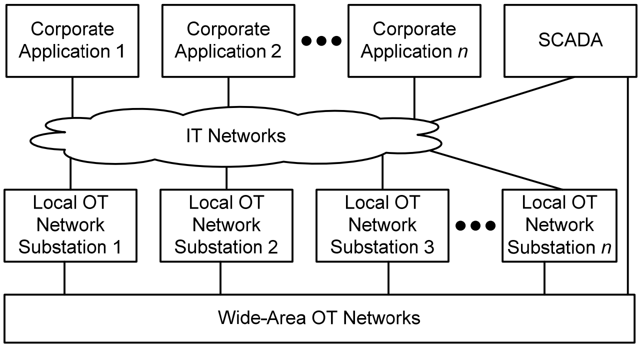
Corporate Application 1
Corporate Application 2
Corporate Application *n*
SCADA
IT Networks
Local OT Network Substation 1
Local OT Network Substation 2
Local OT Network Substation 3
Local OT Network Substation *n*
Wide-Area OT Networks

Fig. 2. Application Example of Wide-Area OT and IT Networks Connected to Substations

X. Testing Demonstrates That Understanding First Principles of Ethernet Improves First Response

With a thorough understanding of the first principles of Ethernet, dependable, secure, and deterministic mission-critical applications have been built with Ethernet. Tests were performed to demonstrate the true impact of poorly designed Ethernet ICT networks on PCM peer-to-peer communications [13]. ICT Ethernet networks were staged with and without the use of best engineering practices. Peer-to-peer communications with several PCM IEDs from different manufacturers were tested on these networks.

One test category was peer-to-peer communications with third-party PCM IEDs with poor implementation of Ethernet first principles. With minimal message traffic, the IEDs occasionally showed appropriate application speed, but they also frequently showed delayed response. Intermittent or persistent degradation of message delivery over casual Ethernet is the exact behavior that designers frequently ignore or, worse, accept. As mentioned, the alarming trend is that designers fail to see these delays as near misses of critical systems and instead see them as a sign of network resilience. When more message traffic was added to the network, performance became worse. These tests confirmed that IED performance changed from a 4-millisecond data exchange between peers to well over 2 minutes. Other tests show that these IEDs will occasionally stop exchanging data altogether with sufficient message traffic on the Ethernet network. These tests prove that frequently used casual Ethernet network design plays a role in the delayed impact of latent defects in these systems.

Tests also show that very specifically designed PCM IEDs, with thorough understanding of Ethernet first principles and deployment of the previously mentioned enhancements, do not experience degraded communications performance. These IEDs continue to exchange information among peers in less than 4 milliseconds, regardless of their messaging configuration. Further, these IEDs continue to exchange information among peers in less than 4 milliseconds, regardless of how much message traffic is added to the network.

XI. Silence Is Not an Option

Testing and observation demonstrate that poorly applied Ethernet technology exhibits message latency and dropped packets. These latent errors often exist for long periods of time before they combine with an event that produces a significant failure, such as a turbine vibration, oil well blowout, or power system apparatus failure. Whether this combination converts a malfunction into a catastrophe often depends on chance. Therefore, it is not prudent to expect to be able to predict or control the malfunction. It is imperative to not ignore Ethernet indeterminism during network design or system acceptance.

Instead, networks with intermittent latencies and dropped packets should be detected and corrected before circumstances allow them to create a crisis.

Columbia University sociologist Diane Vaughan, author of *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*, coined the phrase “challenger launch decision” to describe the organizational behaviors that allowed a frequently observed and glaring mechanical anomaly on the space shuttle to gradually be viewed as a normal flight risk [12]. In the end, a second challenger launch decision by NASA 16 years later to ignore foam insulation near misses on the *Columbia* doomed the crew of yet another shuttle mission.

Another cognitive error is the so-called outcome bias. When people observe successful outcomes, such as launches in the presence of the flaw or message delivery with frequent degradation, they tend to focus on the results more than on the (often unseen) complex processes that led to them. Now, Edward Rogers, the chief knowledge officer at the NASA Goddard Space Flight Center, has instituted a “pause and learn” process in which teams discuss what they have learned at each project milestone. Each mishap is examined, and they also expressly examine perceived successes and the design decisions considered along the way. In this way, teams avoid outcome bias and are more likely to see near misses for what they are.

Near misses can be averted and malfunctions detected prior to catastrophe, but failure is imminent if people are not motivated to reveal near misses or are actually discouraged to do so.

Political scientists Martin Landau and Donald Chisholm described an example that is quite relevant in that it illustrates both the need and hesitation to speak out [12]. Although it took place on the deck of a warship, it is relevant to any organization and any situation where progress in spite of near misses is frequently considered success instead of a signal for alarm. An enlisted seaman on an aircraft carrier discovered that he had lost a tool on deck during a combat exercise. He knew that admitting the mistake could bring a halt to the exercise—and potential punishment—but, more importantly, that an errant tool could cause a catastrophe if it were sucked into a jet engine. Each successful takeoff and landing would be a near miss, a lucky outcome, as long as the tool was missing. He reported the mistake, and the exercise was stopped at significant cost because all aircraft that were aloft were redirected to bases on land. The seaman was commended by his commanding officer in a formal ceremony for his bravery in reporting the malfunction and averting catastrophe.

Leaders in any organization should encourage uncovering near misses—including their own. ICT designers and users should demand appropriate network design and performance for mission-critical communications rather than casual complacency.

It is incredibly rare that ICT networks are for the sole purpose of asynchronous access of inconsequential data. It is more likely that they support some mission-critical application or, equally important, they will be called upon to do so in the future. Therefore, do not be silent—design, or demand from others, ICT designs with sufficient dependability and security technology to demonstrate performance. Do not guess.

If message delivery delays are noticed within networks, do not be silent—ask questions about present and existing applications. Make others aware of the design or performance shortcomings before a malfunction causes a critical problem. Lack of evidence of near misses does not mean they do not exist; it simply means they have not been observed. Better yet, actively find near misses and root them out.

XII. Conclusion

The single greatest engineering achievement of the twentieth century was electrification. This forever changed the world and enabled other top engineering achievements. The first decade of the twenty-first century included numerous major disturbances of the power grid, power plants, offshore microgrids, and power system apparatus. We need to ensure that the second decade ushers in well-engineered modern solutions based on secure and deterministic digital communications. Degraded performance of ICT networks based on shared bandwidth techniques of Ethernet and MPLS must be observed, alarmed, and replaced. ICT designers must understand the fundamental first principles of Ethernet and MPLS to use them dependably and securely.

In fact, IT and OT ICT network designers must collaborate to address completely different expectations for similar acceptance criteria terms of dependability and security.

A decade of Ethernet enhancements to both PCM IEDs and network switches and routers has failed to prevent dropped packets. Within Ethernet networks, delayed and dropped messages will happen. Also, PCM IEDs present the unique problem that they do not require traditional trunk or edge connections to the network, but rather something new that creates confusion for IT experts. Tests demonstrate the degradation of application performance and eventual failure if near misses are ignored and networks are not designed to meet mission-critical standards. However, tests also show that when designed appropriately, with PCM IEDs designed with knowledge of the fundamental first principles of communications, Ethernet can behave in a deterministic, dependable, and secure manner. Designers, consultants, integrators, manufacturers, and end users are duty bound to understand and deploy best engineering practices to maintain the safe and reliable delivery of electric power. Recall that the adoption of Ethernet does not eliminate the requirement to think before connecting. Physical craftsmanship has been replaced by sophisticated network engineering based on IEEE, IEC, and other standards.

Carefully and appropriately designed Ethernet networks make common sense, and it is imperative to make common sense common practice. Identifying near misses and correcting root causes are not only good practice, but are the obligations of designers, consultants, manufacturers, and integrators.

OT and modern IT networks need to be engineered, not simply assembled. IT experts need to be familiar with the following important facts:

- PCM IEDs are peripheral devices that are VLAN aware.
- PCM IEDs that manage IEEE 802.1 QVLANs require a new category of switch connection for a peripheral device with more network control than an edge, such as VLAN management, but not all features expected for a trunk.
- IEC 60834-1 defines latency, dependability, and security requirements.
- Protection-class application dependability and security require near-zero message loss, not buffer and resend.
- PCM networks have static configurations, device addressing, and limited multicast routing—dynamic reconfiguration is not acceptable.
- Failure to address the root cause of Ethernet packet loss has burdened peripheral devices with numerous recovery processes.
- Every dropped packet is a near miss. Each near miss has the potential to overlap message delivery of a malfunction and delay prevention of a catastrophe.
- IT, OT, and PCM experts need to continue to collaborate on appropriate solutions for all applications.
- A single four-layer Internet model network will not satisfy Layer 2 multicast based on the seven-layer OSI model.
- IP QoS and low latency queuing actually provide a different class of service; they do not improve quality of service via dedicated bandwidth.
- Failure and rerouting times between switches are interesting, but the critical measure is time to restore communications to the peripheral devices.

XIII. References

[1] G. Constable and B. Somerville, *A Century of Innovation: Twenty Engineering Achievements That Transformed Our Lives*, Joseph Henry Press, 2003.

[2] M. Panteli and D. S. Kirschen, "Assessing the Effect of Failures in the Information and Communication Infrastructure on Power System Reliability," proceedings of the IEEE Power and Energy Society Power Systems Conference and Exposition, Phoenix, AZ, March 2011.

[3] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal, "Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance," *IEEE Transactions on Power Systems*, Vol. 20, No. 4, November 2005, pp. 1922–1928.

[4] U.S.–Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, April 2004. Available: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

[5] M. Sforna and M. Delfanti, "Overview of the Events and Causes of the 2003 Italian Blackout," proceedings of the IEEE Power and Energy Society Power Systems Conference and Exposition, Atlanta, GA, October 2006.

[6] Union for the Coordination of the Transmission of Electricity, "Interim Report of the Investigation Committee on the 28 September 2003 Blackout in Italy," October 2003.

[7] Ofgem (Office of Gas and Electricity Markets), "Report on Support Investigations Into Recent Blackouts in London and West Midlands," Main Report, Vol. 1, February 2004.

[8] D. Dolezilek, B. MacDonald, J. Kraft, and P. Dolezilek, "In the News: Recent Security Failures Prompt Review of Secure Computing Practices," proceedings of the Protection, Automation and Control World Conference, Dublin, Ireland, June 2011.

[9] D. Dolezilek, N. Fischer, and R. Schloss, "Case Study: Dramatic Improvements in Teleprotection and Telecontrol Capabilities Via Synchronous Wide-Area Data Acquisition," proceedings of the Protection, Automation and Control World Conference, Dublin, Ireland, June 2011.

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

[11] IEEE Power System Relaying Committee Working Group I3, "Transmission Protective Relay System Performance Measuring Methodology," September 1999.

[12] C. H. Tinsley, R. L. Dillon, and P. M. Madsen, "How to Avoid Catastrophe," *Harvard Business Review*, April 2011. Available: http://hbr.org/2011/04/how-to-avoid-catastrophe/ar/1.

[13] 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.

XIV. Biography

David Dolezilek is the technology director of Schweitzer Engineering Laboratories, Inc. He is an electrical engineer, BSEE Montana State University, with experience in electric power protection, integration, automation, communication, control, SCADA, and EMS. He has authored numerous technical papers and continues to research innovative technology affecting the industry. Dolezilek is a patented inventor and participates in numerous working groups and technical committees. He is a member of the IEEE, the IEEE Reliability Society, CIGRE working groups, and two International Electrotechnical Commission (IEC) technical committees tasked with global standardization and security of communications networks and systems in substations.

20120223 • TP6541-01