Defining and Designing Communications Determinism for Substation Applications

Dorran Bekker
e-LEK Engineering

Timothy Tibbals and David Dolezilek
Schweitzer Engineering Laboratories, Inc.

Presented at
GRIDTECH 2015
New Delhi, India
April 8–10, 2015

Originally presented at the
40th Annual Western Protective Relay Conference, October 2013

Defining and Designing Communications Determinism for Substation Applications

Dorran Bekker, *e-LEK Engineering*
Timothy Tibbals and David Dolezilek, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—The bandwidth-sharing nature of Ethernet makes many protection and control engineers uneasy about applying Ethernet for mission-critical protection functions such as tripping, interlocking, or sending permissive or blocking signals. Resolving the determinism question for Ethernet networks in substation protection and control schemes is the single critical factor for further adoption of Ethernet in protection. Consider a simple bus blocking scheme with a blocking signal sent over Ethernet—how should the user set the coordinating timer? What is the worst-case message delivery time given the network design? How should the protection engineer ensure that this time does not change with network expansion or upgrades? How should the protection engineer anticipate the worst-case message delivery time? These questions may seem secondary to communications engineers but are extremely important to protection engineers.**

Message delivery is affected by both frequent and infrequent changes to transfer latency. Real-time intelligent electronic device (IED) processing and Ethernet switch management issues frequently affect the latency of packet delivery. These issues need to be understood and managed to keep the maximum latency of data exchange below the threshold of application failure. Other issues associated with functionality and availability of network devices are less frequent but no less important. Network device unavailability due to failure, repair, or replacement has less frequent but dramatic impact on message delivery. Reliability and longevity information about these network devices must be considered during the design phase. A network used for protection often has more strict availability requirements than a network used for supervisory control and data acquisition (SCADA) or engineering access. It is important to carefully engineer new networks with packet delay latency in mind. It is also important to evaluate existing networks performing less critical tasks when adding new mission-critical messaging.

International standards are used to specify acceptance criteria for the Ethernet network and methods used to satisfy the protection application. This paper discusses different performance criteria for speed, reliability, dependability, and availability. Using these criteria, protection engineers specify the behavior they require for the application and network designers select the technologies and implementation to satisfy the requirements.

I. Introduction

Communications failures were the third most common cause of protection system misoperations in 2011 according to the North American Electric Reliability Corporation (NERC) [1]. The first most common cause was incorrect relay settings, and the second was hardware failure of electromechanical relays. Of the 812 misoperations identified in the second quarter of 2011, 95 percent resulted in unnecessary trips. As communications-assisted protection becomes more prevalent in electric utility and industrial applications, communications networks must be carefully designed to perform correctly.

Modern electric power substations use both serial and Ethernet communications networks. These networks support supervisory control and data acquisition (SCADA) and engineering access, as well as peer-to-peer communications for protection and control applications. Designing communications-assisted protection and control schemes requires thorough understanding of both the data transmission media and protocols. International standards, such as IEC 61850, define various message performance classes that provide guidelines for transmission times of digital messages. Message transport through the network must be able to meet application requirements for delivery and availability during normal and unanticipated conditions.

Serial communication comes with a very high inherent determinism via exclusive use of the channel or via the time-division multiplexing (TDM) of message streams over a physical private network (PPN). These private networks include direct cables and synchronous optical network (SONET) circuit connections that provision their entire bandwidth for a single purpose or path. By not sharing bandwidth, these methods provide time-deterministic message delivery without interference from other unwanted messages.

Most often, however, Ethernet is deployed via indirect connections to one or more switches, rather than directly to the destination device. Messages are sent to addresses within an Ethernet switch network, in order to support numerous simultaneous data paths. Switched Ethernet communication is based on segregating communications connections into multiple coexisting logical channels. For each logical channel, message streams are divided into multiple consecutive packets to better share the network bandwidth. Therefore, Ethernet communication involves receiving, buffering, prioritizing, and forwarding message packets within the network. This, in turn, creates the concern of determinism in message delivery over Ethernet.

II. Defining Determinism for Communications-Assisted Protection and Automation Schemes

Deterministic communication is the ability to consistently transfer data packets across a specified communications channel with predictable end-to-end variation. The variation between packets is called jitter or packet delay variation (PDV). IEC 61850 Protection Class 2 or 3 messages need to be delivered in less than 3 milliseconds, regardless of quantity,

frequency, or network configuration [2], 99.99 percent of the time [3]. This prescribes a PDV budget of much less than 3 milliseconds. The actual PDV budget is 3 milliseconds minus the processing time of the sending and receiving intelligent electronic devices (IEDs), so it is often less than 1 millisecond. During an Ethernet network failure and recovery, mission-critical applications do not allow more latency than 18 milliseconds. This 18-millisecond maximum message transfer latency is required to have a maximum application latency of 20 milliseconds. For example, consider an intertripping scheme operation requirement of 20 milliseconds. When performed by a relay with a 2-millisecond operating cycle, this leaves a PDV budget of less than 18 milliseconds. Less mission-critical applications may endure larger PDV. This must be specified as part of the acceptance criteria for the Ethernet design.

One challenge when discussing deterministic communication is that we cannot limit the discussion to only the communications channel. The IEDs at each end of the communication must also be included in the analysis. They complete the action or process intended by the data being transferred, and so the application cannot be guaranteed deterministic unless the complete process is considered. In this case, we must account for the communications processing delays as well as the process intervals used for logic resolution within the IED. Both the sending IED and receiving IED contribute to these times.

The primary communications media we use today for electric substation applications are serial (EIA-232 and EIA-485) and Ethernet. However, these are standards for the physical layers of these communications methods. On top of these physical layers are the protocols that are chosen to drive the applications. Several of the protocols that are used today are MIRRORED BITS® communications, IEEE 1815 (DNP3), and the protocols within the IEC 61850 communications standard.

The use of these protocols can be broken down into two categories: peer-to-peer and client-server. Each of these communications categories serves different applications with different communications requirements. Peer-to-peer communication is typically used for protection and high-speed automation applications. Client-server communication is used for automation without tight response time requirements, SCADA, and commanded control applications. Depending on the protocol used and the communications channel available, these two classes of applications can use the same channel. It has been shown that digital communication reliably replaces the traditional direct wiring approach for applications such as interlocking between relays [4]. Rather than discuss installation examples, this paper describes the operational technology (OT) rules and tools available to design and implement deterministic digital messaging for these applications.

III. OPERATIONAL TECHNOLOGY VERSUS INFORMATION TECHNOLOGY

Business system experts have collaborated over the last two decades to create a set of services to support the software and communications needs of businesses, generically referred to as information technology (IT) [5]. To many, IT is synonymous with using Ethernet and Internet technologies to move personal and business information. In electric power systems, OT networks are specialized networks that include IEDs that perform protection, control, and monitoring (PCM) applications. Requirements for determinism, dependability, security, and reliability are very different between IT and OT systems and applications.

The Information Technology Infrastructure Library (ITIL®) [5] is a set of practices for IT service management that describes standardized procedures, tasks, and checklists that are not specific to an organization. Previously, OT had little resemblance to IT systems in that OT consisted of isolated systems running proprietary control protocols using specialized hardware and software with predominantly EIA serial connections. Protection, control, automation, monitoring, and communications experts at electric utilities and product manufacturers have successfully collaborated over the last five decades. They created a set of standard services to support the EIA information and control technology (ICT) needs of OT systems.

In the early 1960s, a standards committee, known today as the Electronic Industries Alliance (EIA), developed a common interface standard for data communications equipment. The standard was needed to ensure reliable communication and enable the interconnection of equipment produced by different manufacturers. Thus, the RS-232 standard was born [3]. It specified signal voltages, signal timing, signal function, a protocol for information exchange, and mechanical connectors.

The methods for deterministic EIA serial digital messaging are very mature and documented by the American National Standards Institute (ANSI), which accredits EIA standards. These documented methods essentially represent the universal OT methods similar to ITIL and are not specific to any organization. OT methods for the standardized use of Ethernet are less mature but equally important.

The electric power industry continues to participate in standards organizations to create OT practices that are not specific to any organization for successful ICT in electric power systems based on Ethernet. The industry has adopted the terms *serial* for EIA serial communications services and *Ethernet* for digital messaging based on Ethernet services. We use this convention in this paper.

Perhaps most important to understand is that OT Ethernet relies on deterministic multicasting of messages, or Ethernet packets, for mission-critical protection functions. These OT messages require specific IEEE Ethernet frame components,

such as Ethertypes, which are different than those in any other industry. IEEE assigned unique Ethertypes to IEC 61850 Generic Object-Oriented Substation Event (GOOSE) and Sampled Value messages [6] for use in power system OT specifically because GOOSE and SV performance must be more precise than IT methods.

Mission-critical OT operations often require true deterministic delivery of every message, every time, on time.

IV. Private Purpose-Built Channels Versus Shared Multipurpose Networks

Modern digital power system communications are based on private and shared connections. Direct purpose-built digital serial protocols, including MIRRORED BITS communications, travel directly between several devices networked together, one after another, via single-purpose serial links.

EtherCAT is another good example of a purpose-built fieldbus protocol specifically designed to incorporate data from many Ethernet nodes into a single message [7]. Individual devices are configured to read and write data from specific regions of a single telegram, which means that the telegram mapping sequence does not require individual messages for each node. Private EtherCAT networks are Ethernet networks that do not share services or bandwidth with other protocols. The fundamental difference between EtherCAT and other Ethernet protocols is that a single EtherCAT frame contains I/O point updates from many devices in a network, not just a single device.

EtherCAT messages were designed to exclusively serve data acquisition and control purposes on a dedicated Ethernet network.

Private EtherCAT messages travel directly between several devices networked together, one after another, via single-purpose Ethernet links. Shared bandwidth Ethernet-based IEC 61850, IEEE C37.118 synchrophasor, and IEEE 1815 DNP3 protocols travel between devices networked together in a multicast fashion over multipurpose links to Ethernet switches. These protocols, Ethernet switching, multicast Ethernet packets, and routable Internet Protocol (IP) communications are among the most widely used standards and technologies. They provide the underlying framework for a strategic integrated substation network in an OT system. These protocols have evolved to address the needs and requirements of the substation environment. They were developed to support the long-term growth and performance needs of digital messaging for the modernization of power system ICT in an organized and cost-effective manner.

Today more than ever, IEC 61850 and other initiatives identify IP and multicast Ethernet as the preferred power system networking technology. IEC 61850 and other initiatives support multipurpose integrated substation network architectures and facilitate data exchange with other groups or organizations. Although they present several challenges, routable protocols were developed so that data could be sent among multiple Ethernet networks, intranets, and public links such as the Internet. They allow packets to be forwarded from one network to another. A routable communications protocol, such as TCP/IP, has a network layer address that contains delivery information. This information allows the message to be forwarded without knowledge of the entire path between the source and the destination. Essentially, these protocols contain the device identifier and network address of the device and share the available bandwidth based on the network and message configuration attributes. This bandwidth sharing is the nature of the nondeterminism that must be minimized for OT applications. Bandwidth sharing is necessary and useful outside of the OT network and for moving OT information within an IT network. However, to minimize the PDV of mission-critical messages within the shared Ethernet network, the entire network needs to be designed to minimize PDV. For example, IT-oriented multiprotocol label switching (MPLS) standards suggest that reconfiguration times, and therefore PDV, of 50 milliseconds are acceptable [8]. While this may be true for IT applications, it is not acceptable for mission-critical OT applications. In order to satisfy OT applications, future implementations of MPLS would need enhanced features, including optimized reconfiguration methods to satisfy 5-millisecond latencies. Modern PCM serial protocols are mature, deterministic, stable, widely supported, and easy to configure. Their simplicity is well suited for substation networks and medium-sized regional systems. Innovative message transfer methods provide the performance of routable protocols with the simplicity of a nonroutable protocol and without the huge bandwidth and processing overhead of routable protocols. EIA serial networks are constructed of multiple PPNs. These PPNs reserve their bandwidth for the single purpose of peer-to-peer data exchange, such as MIRRORED BITS communications, and therefore do not experience the jitter and latency that creates the nondeterminism in shared bandwidth Ethernet [9].

The IEEE 802.1D Spanning Tree Protocol (STP) standard [10] was designed at a time when the recovery of Ethernet connectivity within a minute or so after an outage was considered adequate performance via spanning tree algorithms (STAs). Rapid Spanning Tree Protocol (RSTP; IEEE 802.1w [11]) is essentially a modern evolution of IEEE 802.1D. Some manufacturers, unsuccessful in quickly solving the STA in their products, promote proprietary methods that are not interoperable. RSTP is preferred over proprietary methods, but its performance relies on the proper Ethernet switch design. Use of proprietary methods defeats the spirit and purpose of using international standardized methods within communications networks. New Ethernet switches are designed specifically for the mission-critical messages used in power system protection and automation [12]. They provide superior message segregation and solve the STA via RSTP to provide an alternate path in as little as 5 milliseconds. However, if a message is in transit and if it is in a part of the network affected by a failure during the 5-millisecond recovery time (or longer in other switches), it may be lost. If message repetition does not satisfy the application, other methods, like redundancy protocol and duplicate networks, and the associated cost and complexity need to be considered.

V. Recommended Engineering Criteria

The IEC 61850 Communication Networks and Systems for Power Utility Automation – Part 90-4: Network Engineering Guidelines technical report [2] lists network design considerations. Proposed ICT design criteria for IEC 61850-based substation networks include the following:

- Environmental issues
- Electromagnetic interference (EMI) immunity
- Form factor
- Physical media
- Substation application and network topology
- Network IP address plan
- Logical data flows and traffic patterns
- Latency requirements for different types of traffic
- Performance, including packet delivery
- Redundancy
- Reliability, availability, and maintainability
- Time synchronization and accuracy
- Network management
- Remote connectivity
- Cybersecurity
- Scalability, upgradeability, and future-proof
- Testing
- Cost

Prior to the design, a due-diligence evaluation that the ICT network will meet the required performance and reliability must be performed, and international standard methods should be used.

VI. IEC 61850 Methods of Determining Data Transfer Time

The time duration to create and deliver messages between IEDs via a protocol is the message transfer time, represented in Fig. 1 by $t = t_a + t_b + t_c$ [6]. This standardized method of documenting message transfer is essential to understanding PDV. If the overall transfer time satisfies the application requirements, the PDV is acceptable. If, however, changes in t_b make the transfer time unacceptably long, then the PDV is too large. The time duration to publish information in Physical Device 1, deliver it via a protocol message, and act on it in Physical Device 2 is the information transmission time, represented by $T = t + f_2$. The processing interval in the IEDs, during which they perform protection, automation, metering, and message processing, is represented by f. The information transmission time duration is the time truly useful to the design engineer because it represents actually performing an action as part of a communications-assisted automation or protection scheme. Transmission time, T, is easily measured as the time difference between the accurately time-stamped Sequential Events Recorder (SER) reports in IEDs with synchronized clocks. Individual device processing obviously affects the overall application performance. However, PDV is affected by both the message and network design, which affect the delay and variability of the message navigating the network. Also, the receiving IED is affected by the processing variability introduced by message construction, message segregation and prioritization, and unwanted messages. Together, burden from these must not increase the total transfer time beyond 3 milliseconds, per [2].

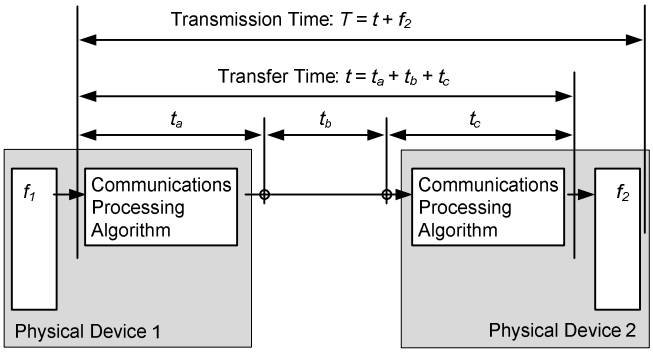

Fig. 1. Data transfer and transmission time

In order to fully evaluate the determinism of a channel, we must also consider the IEDs that are performing the sending and receiving of the data. The basic process is the conversion of the data from processing memory in the IED to bytes of data transmitted on the communications channel, as shown in Fig. 1. This conversion process will be different between the different protocols and communications channels being used. The basic communications processing algorithms are similar for both serial EIA-232 and Ethernet peer-to-peer communications. However, serial messages via direct, private, nonshared bandwidth require much smaller message overhead than Ethernet messages that must navigate indirect, shared bandwidth. The IED design must accommodate the larger message overhead, which requires much more processing.

For a timing example, consider the serial peer-to-peer Mirrored Bits communications protocol, which exchanges Boolean and analog data, encoded in a digital message, between two devices. This messaging technology is used around the world in numerous protection, control, automation, and monitoring applications [9]. The logic points used in the Mirrored Bits communications message are translated into bits in the bytes transmitted in EIA-232 communications. The transmitting IED processes these bits during each logic processing interval, which becomes a factor in determining the overall application process time, along with the communications time between the IEDs. The inherent security feature of the Mirrored Bits communications messaging repeats the bits multiple times to prevent possible data corruption during transmission from being accepted as valid data in the receiving IED. Ignoring the transmission time of the wire or fiber between IEDs, the data transfer time becomes the processing interval of the IED plus the EIA-232 data rate of transmission used in bits per second. The encoding used in Mirrored Bits communications transmits 4 bytes of data per message. Years of field experience have verified the transfer time of Mirrored Bits communications to typically be 3 milliseconds.

VII. Deterministic Message Transfer

Typical GOOSE message publication rates on switched Ethernet networks change to be more frequent as data change. This means nondeterministic transfer of information and possible delays in detection of link failure based on message receipt. GOOSE messages use dedicated virtual local-area networks (VLANs) via unique Ethernet message types and Ethernet frame navigation information on a local-area network. Because of message navigation configuration information, GOOSE message overhead is larger than that of engineered protocols, which reduces the available frame allocation for the payload. This larger message overhead creates inefficient use of communications bandwidth. However, the message navigation parameters allow other message types to use spare bandwidth within the shared bandwidth connections and improve the efficiency of the network.

GOOSE messages are designed to constantly change in size based on changing navigation parameters, support a range of payload sizes, and publish at varying rates. These attributes cause GOOSE messages to use constantly changing amounts of bandwidth in exchange for this flexibility. Content type and changes in the GOOSE contents affect the processing for publishers and subscribers. Changing analog data within a GOOSE message will cause more processing than status data. Also, these changes may affect the time to process the message and therefore impact the PDV. Mission-critical messages must keep the payload variation to a minimum in order to reduce PDV. When possible, transmitting Boolean data only keeps message fluctuation to an absolute minimum.

VIII. International Communications Standards Describe Network Performance Criteria

Risk analysis associated with unwanted events drives the acceptance criteria for each application that the network will support. The performance required for the communications network depends on the accepted level of risk should an unwanted event occur. Power system malfunctions may become technical catastrophes if the protection and automation schemes fail to mitigate correctly. These are called high-impact, low-frequency (HILF) events [13]. However, designers who have never witnessed an HILF event may prioritize the low frequency, rather than the high impact, and allow unacceptable risk.

The result of risk analysis of ICT packet delivery success will influence the level of reliability, dependability, and availability to allocate to each part of the system. For applications that rely on digital messaging to support communications-assisted schemes, risk analysis must consider the following for the communications interfaces, devices, and networks:

- Dependability. The required behavior of a communications-assisted system upon a failure of one of its parts depends on the consequence of that failure. A common criterion for mission-critical protection and automation is *N – 1*, meaning that complete functionality is sustained when any single component fails. The *N – 1* requirement applied to the network as a whole indicates that the network functionality is maintained in spite of any single failure and that it functions correctly because unintended operations are as much or more of a safety issue as a failure to operate.
- Reliability. Designers generally prescribe reliability as a measure of availability values for devices as well as entire systems. Fault tree analysis [9] and other tools help predict the availability of systems based on the availability and interaction of the system components.
- Recovery time. Communications-assisted schemes have a maximum time to reconfigure communications after a failure that the application can tolerate. Failure to deliver in time because of traffic congestion or network failure is both a performance and a security issue. Recovery from a failure needs to be brief enough to not delay a GOOSE or Sampled Value message beyond the application critical threshold. This recovery time must be calculable, measurable, and low enough to meet IEC 61850-5. Due to heavy IT influence in Ethernet design, network recovery time is the OT requirement that is least understood and most difficult to verify. This paper illustrates the need for new design focus, research, and technology to illustrate and satisfy the differences between acceptable IT PDV and OT PDV.

As previously mentioned, deterministic communication is the ability to consistently transfer data packets across a specified communications channel with predictable and measurable end-to-end variation or PDV. Many international standards influence the design of OT systems, and they are summarized in this section to characterize the acceptance criteria for message behavior, application performance, and therefore PDV.

Some of these details describe the IED functional capabilities necessary to satisfy system requirements that are not mandatory for IEC 61850 conformance but are necessary to satisfy the required functionality of the ICT network. IEC 15802 and IEEE 802.1 refer to Ethernet packet construction and delivery used for GOOSE and do not apply to Mirrored Bits communications. However, the other standards listed below address performance without regard for which protocol or network is used. Generally, it is accepted that the performance requirements that do not specify a particular protocol are applicable to both Ethernet and serial messages and protocols. IED communications need to support the functionalities itemized in the following subsections to reduce PDV and provide acceptable message exchange determinism.

A. Instantaneous Communication of Change-of-State Information (IEC 61850 and IEC 60834)

IEC 61850-5 states that devices are expected to immediately react to a received GOOSE message. Though no time is specified for message reception processing, transfer times for different message classes are specified. IEC 60834

and IEC 61850 Part 90-4 describe how immediate delivery through the network devices is required to meet mission-critical applications.

B. Data Delivery Speed (IEC 61850)

Each mission-critical OT machine-to-machine, peer-to-peer multicast message defined as IEC 61850 Protection Class 2 or 3 needs to be delivered in less than 3 milliseconds, regardless of quantity, frequency, or network configuration. This prescribes a PDV budget of 3 milliseconds shared among the processing within the source and destination IEDs and the network devices in between.

C. Message Delivery Performance Requirements (IEC 61850, IEC 60834, IEC 15802, and IEEE 802.1)

Specific message delivery behavior is described by these standards in order to satisfy the data delivery times described in the IEC 61850 standard. They explain network packet delivery performance, t_b in Fig. 1, as a subset of the total PDV budget.

D. Message Delivery Latency (IEC 61850, IEC 60834, IEC 15802, and IEEE 802.1)

IEC 61850 specifies performance classes for message transmission, including the most stringent at 3 milliseconds. IEC 15802 and IEEE 802.1 explain methods to deliver messages and reduce message transmission latency. Permissible latency is referenced by IEC 60834-1, which describes the dependability and security performance requirements for communications systems as part of teleprotection. It references 15-millisecond maximum message delivery latency and 20-millisecond application latency for the permissive tripping teleprotection function and 25-millisecond maximum message delivery latency and 30-millisecond application latency for direct tripping. Some end users have even more stringent requirements of a single power system cycle, or approximately 16-millisecond application latency with an 11-millisecond maximum message delivery latency.

E. Message Delivery Security (IEC 61850 and IEC 60834)

IEC 61850 defines how each received message must be identified as being from the correct source before being acted on. Security defined by IEC 60834-1 indicates the acceptable number of unwanted messages, including wanted but corrupted messages and messages from a source that the receiver is not expecting. Both may unintentionally cause an unwanted operation. Typically, GOOSE messages are exchanged between devices every second. In order to support the intertripping teleprotection function, the requirement is that each IED receive less than nine unwanted messages in a 24-hour period [14]. Therefore, each source IED must deliver no unwanted GOOSE messages and the Ethernet network must not store and forward any unwanted GOOSE messages, including legitimate but delayed messages. Table I illustrates applying the probability of receiving an unwanted command to a GOOSE protection exchange that repeats once a second. The message exchange of once a second is essentially a heartbeat function to constantly validate the health of the channel. Interrupt-driven trip or block functions result in three to eight additional messages published immediately and asynchronously. These messages do not statistically change the number of messages in a 24-hour period.

TABLE I
IEC 60834 SECURITY REQUIREMENTS:
1-SECOND CYCLICAL MESSAGE PUBLICATION

Protection Scheme	Probability of an Unwanted Command P_{uc}	Unwanted Messages Allowed in 24 Hours
Blocking	$< 10^{-3}$	< 86
Permissive Underreach	$< 10^{-2}$	< 864
Permissive Overreach	$< 10^{-3}$	< 86
Intertripping	$< 10^{-4}$	< 9

F. Message Delivery Dependability (IEC 61850 and IEC 60834)

IEC 61850 defines message delivery methods to be used to meet the expectation that each published message is delivered from the source to each intended destination. It also explains methods, such as retransmission, to overcome individually dropped or delayed packets. Dependability defined by IEC 60834-1 indicates the acceptable number of delayed or dropped messages because they may prohibit communications-assisted operations. For a GOOSE exchange between devices, a 1-second heartbeat interval is typical to ensure quick detection of a failure. When this heartbeat is used to verify the health of an intertripping channel, the requirement is that the Ethernet network delay or drop less than one (essentially zero) message to each IED. Table II illustrates applying the probability of missing a wanted command within a GOOSE protection exchange that repeats once a second. This scheme must dependably act each time it is needed and perform a breaker trip when required, with no exceptions.

TABLE II
IEC 60834 DEPENDABILITY REQUIREMENTS:
1-SECOND CYCLICAL MESSAGE PUBLICATION

Protection Scheme	Probability of a Missed Command P_{mc}	Dropped or Delayed Messages Allowed in 24 Hours
Blocking	$< 10^{-4}$	< 9
Permissive Underreach	$< 10^{-7}$	< 1
Permissive Overreach	$< 10^{-7}$	< 1
Intertripping	$< 10^{-8}$	< 1

G. Availability Requirements (IEC 61850, IEC 60834, and IEEE 802.1)

Many OT processes are continuous in nature. Unexpected outages of systems that control industrial processes are not acceptable. Outages often must be planned and scheduled days or weeks in advance. Exhaustive predeployment testing is essential to ensure high availability for OT. Also, many

control systems cannot be easily stopped and started without affecting production. Therefore, to satisfy mission-critical applications, network outages must be resolved in a matter of a few milliseconds and IEDs and switches must have high mean time between failures (MTBF). Less critical applications will endure longer periods of reconfiguration defined by the transfer time of the performance class. High availability of IEDs and systems must be measurable and verifiable in service and is predicted by the high MTBF of devices and fast failover or reconfiguration of the communications network if a system fault should occur.

H. Risk Management Requirements (NERC PRC-005, IEEE 1613, and IEC 61850)

For an OT system, the primary concerns are human safety and fault tolerance to prevent loss of life or endangerment of public health or confidence. Also, if the products and systems in the OT network are out of service, packet delivery is suspended or delayed, which affects PDV. Other concerns include loss of equipment, loss of intellectual property, or lost or damaged products as well as the ability to demonstrate regulatory compliance. The personnel responsible for operating, securing, and maintaining OT must understand the important link between safety and security. Products and systems must meet NERC PRC-005, IEEE 1613, and IEC 61850 reliability requirements.

I. Architecture Security Focus (NERC PRC-005, IEEE 1613, and IEC 61850)

For OT, edge devices (e.g., protective relays, programmable automation controllers [PACs], operator stations, and distributed control system controllers at the perimeter of the network) need to be carefully protected from cyberintrusion. Because they are directly responsible for controlling the end processes, cyberintrusion may render them unable to deliver or act on message packets. They need to be dependable and available when called upon to perform a control action. The protection of the central server is also very important in an OT system because the central server could possibly adversely impact every edge device. Routers, switches, and multiplexers use OT routing information within the network layer addressing to route messages. When positioned at the intersection of OT and IT networks, these devices act as intersection devices. Routers, switches, and multiplexers are edge devices that must satisfy OT and act as perimeter intersection demarcation devices. If these devices are out of service, packet delivery is suspended or delayed, which affects PDV.

J. Physical Interaction (NERC PRC-005, IEEE 1613, and IEC 61850)

OT networks have very complex interactions with physical processes and consequences in the OT domain that can affect physical events. All security functions integrated into OT must be tested (offline on comparable OT) to prove that they do not compromise normal OT functionality. Because these devices and functions often reside in the communications path between devices performing control actions, their availability must be verified. If these devices are out of service, packet delivery is suspended or delayed, which affects PDV. The required environmental ruggedness and reliability of communications networking devices installed in OT networks are dictated by standards such as IEEE 1613. All IEDs, including security, communications, and edge devices, must meet stringent temperature, electric shock and noise, and vibration survivability standards.

K. Time-Critical Responses (NERC PRC-005, IEEE 1613, and IEC 61850)

Security measures such as encryption must not adversely affect PDV. Encryption processes that require fluctuating amounts of processing will cause PDV jitter. In OT, automated response time or system response to human interaction is very critical. For example, requiring password authentication and authorization on a human-machine interface (HMI) must not hamper or interfere with emergency actions for OT. Information flow must not be interrupted or compromised.

L. System Operation (NERC PRC-005, IEEE 1613, and IEC 61850)

OT use of computer operating systems and applications does not tolerate typical IT security practices. Legacy systems are especially vulnerable to central processing unit (CPU) and memory resource unavailability and timing disruptions. Centralized emergency control systems and control networks are often complex and require a different level of expertise (e.g., control networks are typically managed by control engineers, not IT personnel). These systems are often called upon to trigger protection trip and block commands over large distances. If the devices are out of service, packet delivery is suspended or delayed, which affects PDV. This and other availability concerns in this paper are specifically listed because they are often overlooked. Existing networks that perform non-mission-critical tasks may not need the same level of availability. However, when considering adding mission-critical applications to these networks, availability must be understood and managed. Software and hardware are more difficult to upgrade in an operational control system network. Demarcation devices must support encryption capabilities, error logging, and password protection so that these activities do not impact peer-to-peer messages.

M. Change Management (NERC PRC-005, IEEE 1613, and IEC 61850)

Removing devices from service to perform code upgrades will render them incapable of transferring messages. The resulting dropped or delayed packets may not even be observed when a multiplexer is removed from service for repair by the IT staff and the OT protection department is not notified. Change management is paramount for maintaining the integrity of both IT and OT systems. Unpatched software represents one of the greatest vulnerabilities in a system. Software updates on IT systems, including security patches, are typically applied in a timely fashion based on appropriate security policies and procedures. In addition, these procedures

are often automated using server-based tools because their potentially negative impact on network and device availability is considered acceptable. Software updates on OT cannot always be implemented on a timely basis because these updates need to be thoroughly tested by the manufacturer of the industrial control application and the end user of the application before being implemented. OT outages often must be planned and scheduled days or weeks in advance. If these devices are out of service, packet delivery is suspended or delayed, which affects PDV. The impact of frequent patch management must be evaluated in the specification stage and mitigated via redundancy or other methods. Also, it is imperative that the personnel responsible for taking communications components out of service notify and schedule outages with the protection department.

The OT system may also require revalidation as part of the update process. Another issue is that many OT systems use older versions of operating systems that are no longer supported by the manufacturer. Consequently, available patches may not be applicable. Change management is also applicable to hardware and firmware. The change management process must be performed by OT staff and requires infrequent patches and upgrades. The system must be designed with contingencies for continued operation during change management maintenance.

N. Component Lifetime (NERC PRC-005, IEEE 1613, and IEC 61850)

The availability of the end devices and the network between them is essential to effective packet delivery to support the application. Product outage for replacement due to obsolescence, even if infrequent, is an HILF network event that affects packet delivery. When these devices are out of service, packet delivery is suspended or delayed. Typical IT components have a lifetime on the order of 3 to 5 years, with the brevity due to the quick evolution of technology. For OT, where technology has been developed, in many cases, for very specific use and implementation, the lifetime of the deployed technology must be 20 to 30 years. During the network design stage, it is important to consider the various life spans of all the components in the application. The impact of more frequent replacement of communications devices must be evaluated in the specification stage and mitigated via redundancy or other methods.

O. Reliability Metrics (IEC 61850, IEEE 1613, and IEC 60870)

As mentioned, the availability of the end devices and the network between them is essential. A product outage for a replacement due to failure is another HILF network event that affects packet delivery. However, when those devices are out of service, packet delivery is suspended or delayed, which affects PDV. IEC 61850-3 and IEEE 1613 discuss system component reliability metrics that are essential because of the nature of networked IEDs being used to design systems of interoperable devices working in a coordinated fashion for mission-critical purposes. IEC 60870 documents methods to measure and calculate the following:

- Reliability
- Availability
- Maintainability
- Security
- Data integrity
- Time parameters
- Overall accuracy

These and other device performance measures are essential information for predicting the performance, functionality, and reliability of designs executed by networked IEDs. No specific performance benchmarks are expected to be met; however, verification and publication of actual performance measures are necessary in order to conform. Using these published performance measures, system integrators are expected to predict the performance and availability of the interconnected IEDs and, thus, the performance of the system. Again, this is rarely done for non-mission-critical applications of Ethernet but is paramount to preventing high-impact unwanted operations. Furthermore, system integrators need to identify suitably reliable devices for specific mission-critical applications. Reliability measures should include, but not be limited to, specific product reliability metrics and a description of how the metrics are calculated or measured. Metrics that are mandatory include the following:

- Specific product MTBF
- Product family MTBF
- Specific product mean time between removal (MTBR)
- Product family MTBR

Reliability data should be based on the actual incidence of field failures for a large population of installed units. If the provided figures are based on actual data, the approximate size of each installed population used as a basis for each value should be indicated.

IX. Best Practices to Achieve Acceptable PDV

The following itemized applications of the standards and technologies within IEDs and the communications network are necessary to reduce PDV and provide acceptable message exchange determinism over Ethernet. Each application references the standard that describes the technology as follows:

- Provide for individual message management with unique multicast media access control (MAC) addresses for each GOOSE message. This will improve packet delivery and processing determinism. Refer to IEC 61850 and IEC 15802.
- Create message segregation via unique VLAN identifiers (IDs) per GOOSE message. This will improve packet delivery determinism. Refer to IEC 61850 and IEEE 802.1.

- Assign a unique application identifier (APP ID) per GOOSE message. This will improve packet delivery and processing determinism. Refer to IEC 61850.
- Match the last octet of the MAC address, VLAN ID, and APP ID. This will improve packet delivery and processing determinism. This is a good engineering practice but is not yet standardized.
- Use message priority tags based on the mission-critical nature of the communications-assisted application. This will improve packet delivery and processing determinism. Refer to IEC 61850 and IEEE 802.1.
- Assign a descriptive, rather than generic, GOOSE ID. This will improve documentation and troubleshooting. Refer to IEC 61850.
- Use a descriptive textual name and VLAN ID. This will improve documentation and troubleshooting. This is a good engineering practice but is not yet standardized.
- Carefully manage the GOOSE application processing at both the source and destination devices via careful design of data set contents and message retransmission properties. This will improve packet delivery and processing determinism. Refer to IEC 61850 and IEC 60834.
- Choose IEDs and switches that immediately publish, transmit, and react to GOOSE messages. This will improve packet delivery determinism. Refer to IEC 61850 and IEC 60834.
- Design Ethernet switch network connections, and determine backup data paths through intentional selection and settings. Use root-plus network design; intentionally select backup root and IED ports based on actual network performance in primary and reconfigured states. This will improve packet delivery determinism. Refer to IEC 61850 and IEEE 802.1.
- Test and verify that Ethernet switches satisfy reconfiguration times of 15 milliseconds. These methods must be based on standardized STAs and RSTP rather than proprietary solutions. This will improve packet delivery determinism. Refer to IEC 61850, IEC 60834, and IEEE 802.1.
- Ensure that mission-critical applications are served by redundant devices as well as redundant communications. This will improve packet delivery determinism in case of failure. Refer to IEC 61850.
- Transport control system communications for the IEC 61850 and IEEE 1815 routable protocols leaving the station via secure nonroutable TDM Epipes to satisfy NERC Critical Infrastructure Protection (CIP). This method also eliminates the nondeterminism of public networks and MPLS. Alternately, the routable protocols must be converted to nonroutable protocols for transport over nonsecure links, and mission-critical applications outside the substation must be derated due to nondeterminism, jitter, and increased message latency. This will improve packet delivery determinism. Refer to NERC CIP, IEC 61850, and IEC 60834.
- Use a unique VLAN ID and MAC address for all network multicast messages. All untagged traffic must be tagged with the same port-based VLAN (PVLAN) at ingress to the Ethernet network. This will improve packet delivery determinism as well as documentation and troubleshooting. Refer to IEC 61850 and IEC 60834.
- Disable all unused IED and switch communications ports. All network engineering ports must have static MAC address filters to prevent all but known engineering laptops. This will improve packet delivery determinism. Refer to NERC CIP and NERC PRC-005.
- Ensure that all IEDs monitor the multicast message sequence number and state number to supervise data exchange via digital messaging. This will minimize the time to detect packet delivery failure. Refer to IEC 61850 and IEC 60834.
- Ensure that all IEDs calculate and publish an accurate time-to-live value within each multicast GOOSE message to allow subscribers to detect a failed digital data exchange as soon as possible. This will minimize the time to react to packet delivery failure. Refer to IEC 61850 and IEC 60834.
- Make sure that all IEDs create GOOSE diagnostic reports that include performance and reliability statistics and real-time operational information for each published and subscribed GOOSE message. This will improve the ability to monitor, validate, and diagnose packet delivery performance. Refer to IEC 61850 and IEC 60834.
- Verify that each IED supervises all GOOSE attributes to detect and alarm abnormal behavior via the front-panel display, SCADA alarms, and direct messaging to technicians. This will improve the ability to communicate packet delivery performance information to those who need to know. Refer to IEC 61850 and IEC 60834.
- Make sure that each IED time-stamps and creates a sequential event record for each GOOSE message failure and then reacts to the failure by modifying logic. Each IED should also alert local and remote applications that communications-assisted data acquisition has failed. This will improve the ability to monitor, validate, and diagnose packet delivery performance. Refer to IEC 61850 and IEC 60834.
- Ensure that all system devices, logic processors, switches, routers, gateways, and annunciators export settings for documentation of an as-built and commissioned system configuration. The system must support automatic verification that system settings have not changed and real-time verification of the health of all source instrument transformers and trip circuits. This will improve the ability to document and

evaluate as-built and commissioned packet delivery systems. Refer to IEC 61850, NERC CIP, and NERC PRC-005.

- Verify that all system devices, logic processors, switches, routers, gateways, and annunciators support configuration via the direct transfer of the IEC 61850 Substation Configuration Language (SCL) file directly into the IED and export it for storage or remote loading. This will improve the ability to be confident that the device configuration matches the engineered design. Refer to IEC 61850, NERC CIP, and NERC PRC-005.
- Make sure that for each IED, the manufacturer provides documentation of interoperabilty certification with devices from numerous other suppliers. Based on user group acceptance of the platform and product family testing, these certificates should reference the testing of the IEC 61850 interface as well as the proven ability to interoperate with other manufacturer devices and configuration files. This will improve the ability to design and build packet delivery systems for use with devices from multiple manufacturers. This is a good engineering practice but is not yet standardized.
- Test the system with commissioning tools to verify the management of VLANs and MAC addresses on every network port, and design the system to support real-time GOOSE monitors to collect and verify Ethernet activity at the IED port. This will improve the ability to test and validate the packet delivery configuration in the as-built and commissioned Ethernet system. This is a good engineering practice but is not yet standardized.
- Design computer-based testing tools to run on operating systems that are more deterministic than those within typical general-purpose products to reduce jitter and timing errors introduced by non-real-time operating systems. Incorrect use of these tools and applications will provide false readings of PDV. Computer testing tools based on an office-grade operating system must include user warnings that time stamps created by the computers are inaccurate and should not be compared and coordinated with real-time time stamps from IEDs. Personal computer time stamps are unpredictable and inconsistently skewed by up to 50-millisecond inaccuracy due to CPU jitter. This means that both relative and absolute time assigned by the computer cannot be relied on. This will improve the ability to test and validate packet delivery systems. This is a good engineering practice but is not yet standardized.
- Ensure that for each IED, the manufacturer provides documentation of IEC 61850-3 metrics of reliability and maintainability, including the method of measurement or calculation. Designing for reliability relies on accurate device and system reliability comparisons. Fault tree calculations and risk analysis rely on accurate and consistent reliability metrics. This will improve the ability to evaluate, design, and document the availability of packet delivery devices and systems. Refer to IEC 61850, IEC 60834, and IEEE 1613. The following metrics should be provided:
  - MTBF, measured in years.
  - Mean time to diagnose (MTTD), measured in minutes.
  - Mean time to repair (MTTR), measured in minutes.

As mentioned, availability of the end devices and the network between them is essential to effective packet delivery to support the application. Incorrect Ethernet network message behavior may cause the failure of Ethernet switch devices. Even if these devices are out of service infrequently due to network traffic, packet delivery is suspended or delayed during that time, which affects PDV. Therefore, another reliability concern is the use by devices of the default PVLAN setting of 1, which is used for switch-to-switch management protocols. As a consequence, use of VLAN 1 may put the network at a higher risk for security attacks from untrusted devices that by misconfiguration, pure accident, or malicious action gain access to VLAN 1 and exploit this security flaw. Also, if VLAN 1 is saturated via some unexpected data storm, it may be impossible to communicate management messages to the switch over the shared VLAN 1 in order to mitigate the problem.

A simple, commonsense security principle recommended by IT professionals is to change the default PVLAN to be something other than 1. For power systems, 1001 is recommended. This keeps user data and protocol traffic separate from network management traffic.

X. Conclusion

When the Ethernet network is a part of the teleprotection or interlocking scheme, it must be specified, designed, and built to satisfy the required performance. Protection engineers identify the typical and maximum times to perform the application. As a subset of the protection actions, the typical and maximum message transfer times between devices are established, as well as how often the transfer time can deviate from the typical. Given this, the network designer establishes the typical and maximum transfer times of packets, as well as the percentage that must meet the typical time. From this, the PDV requirements are established and the system is designed, built, and tested to support them.

This paper explains how to use international standards to identify and specify acceptance criteria for the Ethernet network and the methods used to satisfy the protection application. Protection engineers specify the Ethernet behavior they require to satisfy the requirements for speed, reliability, dependability, and availability.

In Ethernet networks, physical craftsmanship has been replaced by sophisticated network engineering based on IEEE, IEC, and other standards. A decade of Ethernet enhancements to both PCM IEDs and network switches and routers has created methods to help address the challenge of deterministic

message delivery. Within Ethernet networks, delayed and dropped messages will happen. Networks need to be engineered to manage PDV and reliable delivery via these methods as well as application and network redundancy.

When the substation Ethernet network is designed appropriately and includes both the end devices and communications devices designed for PCM performance requirements, Ethernet can behave in an adequate, 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.

IEDs and the communications network need to support the standardized and itemized technologies to reduce PDV and provide acceptable message exchange determinism. OT networks need to be engineered, not simply assembled. This new engineering process includes the following:

- Learning the differences and similarities of OT and IT.
- Understanding the benefits and shortcomings of both time-deterministic EIA serial and SONET channels and nondeterministic Ethernet and MPLS channels.
- Learning methods to reduce or mitigate the nondeterminism inherent in Ethernet and MPLS shared bandwidth technologies.
- Choosing between private EIA serial connections, shared bandwidth Ethernet connections, or a combination of the two to accomplish all local-area network communications applications.
- Determining methods to define, measure, and document data transfer times and identify acceptable packet delay variability.
- Learning the numerous international communications standards that describe the rules and acceptance criteria for communications performance.
- Using the numerous international communications standards that describe the tools to be used within multimanufacturer systems to create and verify acceptable communications performance.
- Designing a communications system that balances the requirements for throughput, speed, reliability, dependability, security, and cost and that clearly demonstrates that PDV is acceptable.

XI. References

[1] J. A. Seidel, "2Q2011 Misoperation Results," presentation in the NERC Industry Webinar, December 1, 2011. Available: http://www.nerc.com/files/misoperations_webinar_master_deck_final.pdf.

[2] IEC/TR 61850-90-4, Communication Networks and Systems for Power Utility Automation – Part 90-4: Network Engineering Guidelines, Technical Report, August 2013. Available: http://webstore.iec.ch/.

[3] TIA-723-1998, High Speed 232 Type DTE/DCE Interface.

[4] G. W. Scheer and R. E. Moxley, "Digital Communications Improve Contact I/O Reliability," proceedings of the 7th Annual Western Power Delivery Automation Conference, Spokane, WA, May 2005.

[5] M. Moussamir and D. Dolezilek, "The Demands and Implications of IT and OT Collaboration," proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2013.

[6] D. Dolezilek, "Using Information From Relays to Improve the Power System – Revisited," proceedings of the 1st Annual Protection, Automation and Control World Conference, Dublin, Ireland, June 2010.

[7] 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 2nd Annual Protection, Automation and Control World Conference, Dublin, Ireland, June 2011.

[8] Cisco, "Extending MPLS Across the End-to-End Network: Cisco Unified MPLS," Cisco White Paper C11-656286-01, 2011. Available: http://www.cisco.com/en/US/prod/collateral/optical/ps5726/ps11348/white_paper_c11-656286.pdf.

[9] M. Gugerty, R. Jenkins, and D. J. Dolezilek, "Case Study Comparison of Serial and Ethernet Digital Communications Technologies for Transfer of Relay Quantities," proceedings of the 33rd Annual Western Protective Relay Conference, Spokane, WA, October 2006.

[10] IEEE Standard 802.1D™, IEEE Standard for Local and Metropolitan Area Networks – Media Access Control (MAC) Bridges, Amendment 5: Bridging of IEEE 802.16.

[11] IEEE Standard 802.1w-2001, IEEE Standard for Local and Metropolitan Area Networks – Common Specification. Part 3: Media Access Control (MAC) Bridges – Amendment 2: Rapid Reconfiguration.

[12] SEL-2730M Managed Ethernet Switch Instruction Manual. Available: http://www.selinc.com.

[13] G. Cauley and M. Lauby, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," 2010. Available: http://www.nerc.com/files/HILF-060210.pdf.

[14] D. Dolezilek, "Ethernet Design for Teleprotection and Automation Requires a Return to First Principles to Improve First Response," proceedings of the 14th Annual Western Power Delivery Automation Conference, Spokane, WA, March 2012.

XII. Biographies

Dorran Bekker received his BSCE in 2007. After working at e-LEK Engineering as an application engineer for a year, he joined Consolidated Power Projects as a SCADA/automation engineer. In June of 2013, he returned to e-LEK Engineering in a new Smart Grid Solutions division.

Timothy Tibbals received his BSEE from Gonzaga University in 1989. After graduation, he joined Schweitzer Engineering Laboratories, Inc. (SEL) as an application engineer, performing system studies and relay testing. Tim has also worked as a development engineer and as part of the development team for many of the communications features and functions of SEL products. He subsequently worked as an application engineer for protection, integration, and automation products, assisting customers through product training, seminars, and phone support. Tim served as the automation services supervisor in the SEL systems and services division for several years before returning to the research and development division as a product engineer for automation and communications engineering products. He is currently a senior automation system engineer in the research and development division.

David Dolezilek received his BSEE from Montana State University and is a research and development technology director at Schweitzer Engineering Laboratories, Inc. He has 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. David 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 the global standardization and security of communications networks and systems in substations.