Improvements in Synchronous Wide-Area Data Acquisition Design and Deployment for Telecontrol and Teleprotection

David Dolezilek, Normann Fischer, and Robert Schloss
Schweitzer Engineering Laboratories, Inc.

Presented at the
Southern African Power System Protection Conference
Johannesburg, South Africa
November 14–16, 2012

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

Improvements in Synchronous Wide-Area Data Acquisition Design and Deployment for Telecontrol and Teleprotection

David Dolezilek, Normann Fischer, and Robert Schloss, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—The operation times of circuit breakers and other primary equipment cannot be shortened and, in fact, may slow as physical attributes affect components in service. Therefore, in order to improve the performance of teleprotection and telecontrol, systems must increase the amount of decision-making information that is communicated while also reducing the transit time. Previous papers have discussed communications channel "throughput" as a function of protocol behavior and available communications channel bandwidth. However, another metric common to other industries and newly recognized by power system protection and control engineers is "goodput." Goodput is the amount of useful data, user data, or payload that can be processed by, passed through, or otherwise put through a system and received at the correct destination address. It is actually application information throughput, a measure of the amount of information exchanged between devices participating in an application, as opposed to traditional communications message throughput. Goodput is a ratio of the delivered amount of information and the total delivery time, minus any packet headers or other overhead and minus any information lost or corrupted in transit. For Ethernet multicast communication, such as IEC 61850 Generic Object-Oriented Substation Event (GOOSE) and the new IEEE C37.238 time-synchronization method, the goodput may need to be calculated without knowledge of packet loss or corruption. In this case, it is a useful metric for identifying optimal scenarios for secure message transfer.**

Goodput, other methods of comparison, and test results are explained in this paper to illustrate the necessary design considerations to improve applications such as teleprotection, telecontrol, and communications-assisted automation. This paper introduces exciting improvements to the state of the art in power system protection, automation, and control via innovative high-speed data acquisition techniques. Microprocessor-based protection, control, and monitoring intelligent electronic devices (IEDs), such as relays, determine power system operating characteristics by performing real-time scaling, calculations, and analytics on data acquired as raw values from direct-wired instrument transformers and the status of contact inputs. If abnormal conditions exist, relays record information, make decisions, and take action. In addition to detecting faults and tripping circuit breakers, the actions include sharing information with other IEDs via digital communications. By performing wide-area decision making with values from other IEDs in other locations, relays are capable of making more sophisticated decisions with knowledge of the characteristics of multiple points on the power system.

Teleprotection algorithms that are improved with digital communications with high goodput include direct underreaching transfer trip (DUTT), permissive underreaching transfer trip (PUTT), permissive overreaching transfer trip (POTT), directional comparison blocking (DCB), directional comparison unblocking (DCUB), and line current differential. Telecontrol applications that benefit from digital communications with high goodput include load shedding, load sharing, generation shedding, islanding detection, intelligent system separation, generation and frequency control, voltage and MVAR control, distribution automation, and automatic network reconfiguration.

This paper compares the improved performance of remote communications-assisted decisions and explains important digital message performance metrics useful in the design and specification of communications channels.

I. Introduction

Localized protection and control functions within modern microprocessor-based relays directly measure the required data representing the present state of the power system, without the aid of communications assistance. This is achieved by performing analog-to-digital conversion on low-level analog signals directly wired into relay input contacts from field contacts and instrument transformers physically monitoring power system apparatus. Communications-assisted localized protection and control functions collect data from a second intelligent electronic device (IED) that measures values associated with other field contacts and instrument transformers. IEDs specialized for power system applications and now migrating to other mission-critical applications are referred to as protection, control, and monitoring (PCM) IEDs because they are designed to do all three functions simultaneously. The values of these field signals from the second IED, as well as other calculated quantities, are acquired as contents of digital messages via various communications mediums. The contents of the digital messages are combined with the local measurements in the relay to provide a larger pool of values to use within protection and automation logic. Presently, the process to move data from a data provider IED to a data consumer IED includes data change detection; message creation, publication, transfer, reception, and verification; and parsing and mapping of message contents into virtual data locations in the relay.

Operational technology (OT) refers to the devices and methods, such as networks of IEDs, used to automatically control and manually operate an industrial process. Whereas information technology (IT) systems move information, OT systems use information, specifically directly between devices. In electric power systems, OT networks are specialized IED networks that include PCM IEDs and associated PCM applications.

II. Digital Messaging

It is important to note that data received via digital messaging represent the present state when they were actually measured or calculated at an instant in the recent past. The latency of the value depends on the message processing and transfer latency. Therefore, these remote values are not from the same instant in time as those presently measured and calculated in the relay from direct field contacts. For applications that require data measured at the same instant in time, such as line current differential, this lack of synchrony, or data incoherence, requires that the relay constantly archive locally calculated values. The relay collects data created at some point in the past from the second IED via a digital message. Then it retrieves the associated archived values that were created locally at the same instant in the past for use together in synchronized logic. This process is referred to as data alignment. The messages must behave deterministically to support data alignment, and the precision of this alignment dictates the types of logic processing possible. If the messaging is not deterministic, data alignment is not possible, which further restricts possible types of logic processing. Dramatic improvements in the availability and accuracy of synchronous wide-area networks (WANs) create a proportional improvement in data acquisition via digital messaging over these networks.

Data acquired through digital messaging between IEDs represent the statuses of apparatus and functions that facilitate effective power system operation. Contemporary microprocessor-based relays routinely communicate metering, protection, automation, control, teleprotection, and telecontrol information that requires the messages to travel from point to point with a high degree of security and dependability.

IEC 60834-1 describes requirements for message propagation time and communications channel reliability [1]. For teleprotection, interlocking, and high-speed automation, message propagation time through the communications channel must be under 3 milliseconds. Also, the teleprotection receiver has a limited time to process received commands. Any unwanted messages delivered to the teleprotection receiver may delay processing or, worse, push a wanted message off of an input queue or buffer so that it is never processed.

Digital messaging between devices is performed using an agreed upon network and protocol. A protocol is a method used over a local-area network (LAN) or WAN to control the connection, communication, and data transfer between devices. The protocol includes message formats, services, procedures, and addressing and naming conventions. Networks include direct serial connections, serial-based LANs, and Ethernet LANs. These networks are built using copper cables, fiber cables, and wireless radio transmissions. The majority of successful substation integration systems being installed today and in the near future are based on non-Ethernet LANs and built using EIA-232 point-to-point communications connections between IEDs and information processors. However, deployment of Ethernet solutions is growing rapidly. WANs interconnect multiple LANs.

A. Standards Development Organizations and Standards-Related Organizations

The National Institute of Standards and Technology (NIST) defines a standardized protocol as one developed by a standards development organization (SDO). The primary activities of a protocol SDO include developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise maintaining protocol definitions. A standards-related organization (SRO) is skilled in the art of protocol development, such as a manufacturer that develops internal protocols and contributes expertise and resources to SDOs.

B. Standardized Protocols

Standardized protocols include IEC 60870, IEC 61850, EtherCAT, and DNP3, each managed by an SDO and/or a users group committee funded by a collection of manufacturers and users that organize enhancements and testing. The protocol SDO and users group work together to create and maintain a set of rules to exchange messages between devices from multiple manufacturers or multiple product lines from the same manufacturer. Therefore, SDOs include communications experts who work together to standardize message formats, services, procedures, and addressing and naming conventions to promote data exchange among multiple manufacturers. System designers then configure the behavior of these standardized protocols and necessary network components to match the application requirements as closely as possible. For telecontrol and teleprotection, the useful peer-to-peer SDO protocols include IEC 61850 Generic Object-Oriented Substation Event (GOOSE) messaging and EtherCAT.

C. Engineered Protocols

Engineered protocols include Mirrored Bits® communications and other open protocols developed by SRO manufacturers to solve specific applications. As microprocessor-based relays evolved to integrate multiple functions into one physical device, several communications protocols were purpose-built by power system experts to solve specific applications. Multiple applications require multiple types of device conversations to move virtually thousands of pieces of information among IEDs. For each application, system designers select the protocol that was designed to specifically perform that application. Then they choose a network to support those protocols. Relay and IED designers combine their skills in the art of protecting and automating power systems with their knowledge of the parameters of IED development [2]. For telecontrol and teleprotection, the frequently used peer-to-peer SRO protocol is Mirrored Bits communications.

D. SDO Protocols Contrasted With SRO Protocols

SDO standardized protocols are designed by communications experts to facilitate data exchange among devices. SRO engineered protocols are purpose-built by power system experts to satisfy PCM applications. Then they are standardized and offered via a reasonable and

nondiscriminatory license by the SRO to facilitate data exchange among multiple manufacturers.

The IED designer must guarantee that each of the following high-priority tasks happens each processing interval within an IED for both SDO and SRO protocols:

- Measurement of inputs
- Calculation of values
- Reception of messages
- Data alignment
- Protection
- Metering
- Archival of information
- Publication of messages

III. Benefits of High-Speed Communication as Applied to Protection Systems

The benefit that communications schemes afford to protection systems is that they provide data from geographically remote terminals to a local terminal, ensuring fast and accurate fault location and detection. The data that are typically transported across the communications network may comprise either digital data (distance protection or remedial action schemes) or a combination of analog and digital data (line differential protection or remedial action schemes). The type of data being transported and the speed at which these data have to be transported across the network primarily dictate the required network bandwidth.

Another important consideration is that these digital communications schemes simplify the trip functions by eliminating physical components, such as breaker failure initiate output contacts to communicate breaker failure over copper conductors, as well as lockout relays. When either of these physical components fails, power system apparatus are damaged or destroyed. Correctly engineered, tested, and commissioned interlock and teleprotection done via digital messaging via Mirrored Bits communications, IEC 61850 GOOSE, or EtherCAT provide higher reliability and security of protection functions.

For the purpose of this paper, we concentrate on line distance protection enhanced with communications-assisted schemes. The data that are communicated from the remote terminals to the local terminal are predominately digital. Distance protection schemes complemented with communications-assisted schemes result in better protection for the entire transmission line. Consider the simple power system shown in Fig. 1. The reaches of Zone 1 (instantaneous underreaching zone), Zone 2 (overreaching zone), and Zone 3 (reverse reaching zone) of the distance elements for the local and remote relays for the protected line (TL1) are superimposed on the power system.

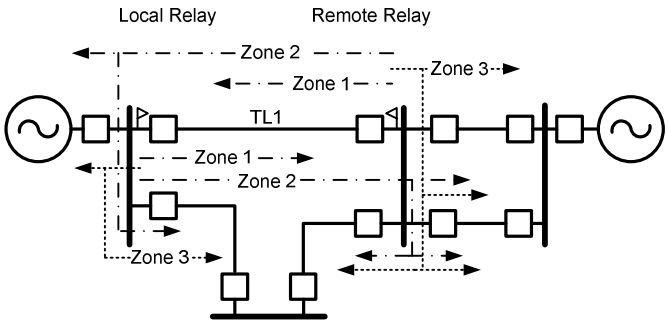

Fig. 1. Sketch of a simple power system with zone reaches superimposed

In Fig. 1, we can clearly see that Zone 1 does not protect the entire transmission line; this is done so that the relay does not trip for faults outside of the protected line due to errors in the instrument transformers or line impedances. Fig. 1 illustrates that Zone 2 not only covers the entire transmission line but also a percentage of the adjacent lines. Zone 2 is set so that it does not assert the trip output instantaneously upon detecting a fault but engages a timer. Only once the timer expires does it assert the trip output. This is done so that the relay closest to the fault has a chance to clear the fault first. The drawback of this approach is that the trip output is delayed for faults that occur inside the protected line but outside of the Zone 1 reach. Protection engineers require that protective devices not only clear system faults as rapidly as possible but also isolate only the affected zones and keep the remaining healthy system connected. To enable rapid detection of transmission line faults that fall outside of the Zone 1 reach, communications-assisted schemes are needed.

Two predominately different communications-assisted schemes exist: permissive and blocking. In a permissive scheme, before the local terminal Zone 2 element is allowed to trip rapidly, it has to receive permission signals from the remote ends [3]. The remote ends use their Zone 2 elements to send the permissive signal. In this manner, all relays that protect the zone agree that the fault is within the protected zone. Fig. 2 illustrates the basic operating principle of a permissive overreaching transfer trip (POTT) scheme.

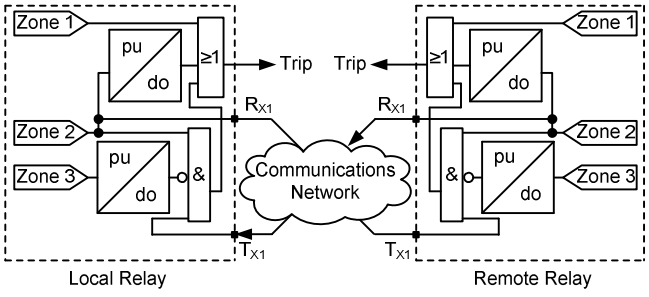

Fig. 2. Simple sketch of a POTT scheme

Fig. 3 shows a directional comparison blocking (DCB) scheme, where the local Zone 2 element starts a timer when it asserts. If the logic does not receive a block signal from the remote terminal before the timer expires, it asserts the trip output. The remote terminals use their Zone 3 elements to send the block signals. Assertion of a remote terminal Zone 3 element verifies that the fault is outside of the protected zone.

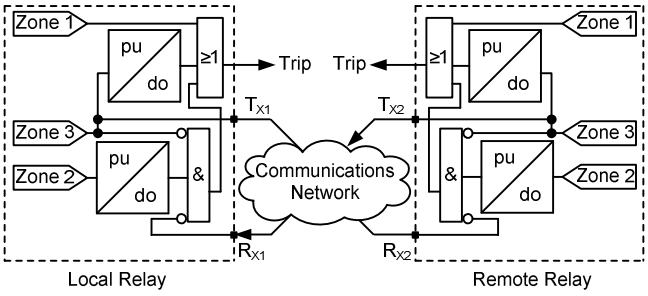

Fig. 3. Simple sketch of a DCB scheme

Either the POTT or DCB scheme can be used to ensure rapid tripping for faults that occur in the region of the line not covered by the Zone 1 distance element.

For both communications schemes, the trip command from the relay for a fault on the line not covered by the Zone 1 element is delayed. The delay time is directly proportional to the time it takes for a data bit from the remote terminals to be sent to the local terminal. Therefore, if the time on the wire plus the encoding and decoding time between the remote terminals and the local terminal can be reduced, the clearing time for any fault on the protected line can be reduced.

Fig. 4 is a timing diagram showing the total fault-clearing time for a fault on the protected line that occurs within the Zone 1 reach of the relay. Notice that the time between the relay detecting the fault and issuing the trip signal is very small (typically 2 to 4 milliseconds).

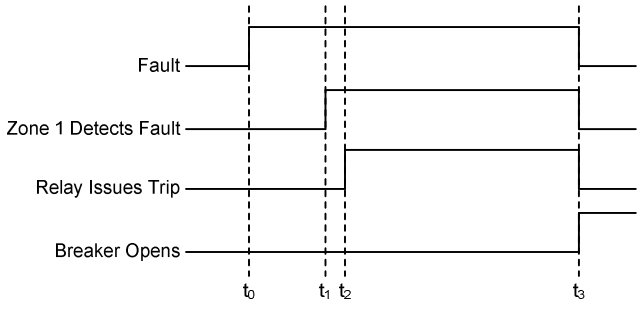

Fig. 4. Timing diagram for a fault within the Zone 1 reach

Fig. 5 is a timing diagram showing the total fault-clearing time for a fault on the protected line that occurs outside of the Zone 1 reach of the relay. Notice that the time between when the relay detects the fault and when the relay issues a trip is dependent on the time it takes for the permissive signal to arrive and be verified. Therefore, there is a direct correlation between the delay in the relay tripping time and the time on the wire of the permissive signal.

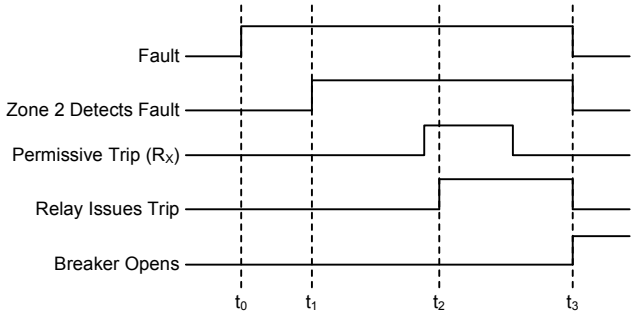

Fig. 5. Timing diagram for a fault outside of the Zone 1 reach

Protection engineers strive to have the timing diagram shown in Fig. 5 closely resemble the timing diagram shown in Fig. 4. In other words, protection engineers like all faults on the protected line to be cleared in Zone 1 time. To achieve this goal, the time to compile, transmit, and verify the permissive message must be driven to the absolute minimum.

The amount of thermal damage caused by a short circuit is directly related to the duration of the short circuit on the power system. Large disturbances on a power system, especially faults with breaker failures, reduce the ability to transmit power between generation and load centers. This reduced transmission capacity results in portions of the power system accelerating and decelerating during a fault, increasing the angular distance between the parts of the system. Shorter breaker failure clearing times minimize the angular distance between the parts of the system, resulting in a lower chance of an out-of-step condition [4]. Total breaker failure clearing time consists of the following parts:

1. Primary relay operate time – time required to initially detect a short circuit on the power system.
2. Breaker failure initiate – time required to send an initiate signal from the primary protective relay to the breaker failure relay.
3. Breaker failure time delay – time required to clear the fault by the circuit breaker and detect open phases. An additional margin of two or more cycles is usually added to this time.
4. Distribution of breaker failure trip – time to send breaker failure tripping signals to local and remote circuit breakers.
5. Circuit breaker clearing time – time required by the local and remote circuit breakers to interrupt the fault current.

As in the previous examples of fault clearing via communicated signals, the latency of Items 2 and 4 within the breaker failure clearing sequence is directly proportional to the time it takes for a data bit to travel between protective devices. The overall improvement of faster communication in a traditional breaker failure scheme has the same effect as replacing older three-cycle circuit breakers with newer two-cycle circuit breakers. This shorter breaker failure clearing time minimizes damage due to breaker failure events

and maintains system stability. The duration of the distribution of the breaker failure trip essentially becomes the transfer time if the relays use high-speed output contacts that operate in microseconds. Therefore, the mission-critical trip function is improved by 300 percent by changing the transfer time from 3 milliseconds to 1 millisecond. This, in turn, reduces the wear on the power system apparatus by reducing the duration of operation under fault conditions by 300 percent.

Communications-assisted protection schemes allow for faster and more secure protection and control of power systems. The increased speed of data transfer afforded by EtherCAT allows systems to operate before additional contingencies cause power system instability. Without this higher speed, more elaborate methods may have to be deployed at each system control point to account for the slower communication. A major benefit of faster communication for power system owners is that equipment is subjected to higher fault current for a shorter duration.

For example, consider a power transformer. High-magnitude currents are known to be a major factor in reducing the life of a transformer [5]. Power system faults external to the transformer zone cause high-magnitude currents to flow through the transformer. These high-magnitude through-fault currents create radial and axial forces within the transformer that force the windings of the transformer against one another. The mechanical force created when windings are forced against one another damages the insulation and reduces the mechanical integrity of the windings. This damage is cumulative, meaning that the longer the fault exists, the more the working life of the winding is reduced. Therefore, reducing the duration of the fault prolongs the working life of the transformer.

IV. Data Transmission Time

Obviously, the efficiency of the reception and publication of messages also directly impacts the quality and quantity of data received through digital communication [6].

The latency of data transfer between the second IED and the relay is determined by the processing of message encoding, transport, and decoding and is not symmetrical. The latency of data-change detection, message creation, and message publication is dictated by the hardware and firmware design of the second IED and how quickly the device performs these functions. The latency of message reception, verification, parsing, and content mapping is dictated by the hardware and firmware design of the relay and how quickly the relay performs these functions.

The time duration to create and deliver messages between IEDs via a protocol is the message transmission time, represented in Fig. 6 by $t = t_a + t_b + t_c$ [7]. 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 transfer 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 transfer 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. Transfer time T is easily measured as the time difference between the accurately time-stamped Sequential Events Recorder (SER) reports in IEDs with synchronized clocks.

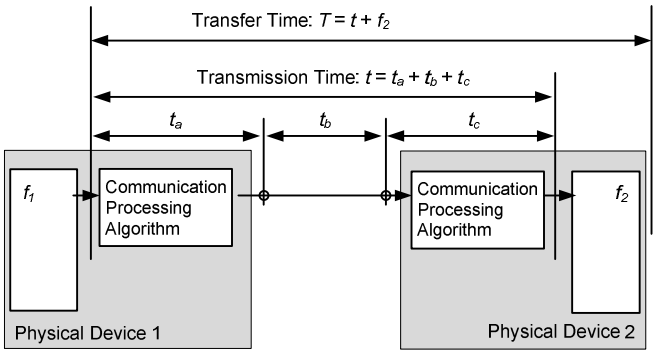

Fig. 6. Transmission time definition [7]

The two most prevalent message technologies in use in the electric power industry today are MIRRORED BITS communications and IEC 61850 GOOSE.

V. MIRRORED BITS COMMUNICATIONS

The MIRRORED BITS communications protocol is a serial communications technology that exchanges the status of Boolean and analog data, encoded in a digital message, from one device to another. It performs the reliable exchange of critical data using a simple and effective method to communicate bits of logical status information between IEDs for protection, control, and monitoring. Each incoming message is made up of logic bits received from a remotely connected IED. At the same time, the receiving IED transmits logic bits to the remotely connected IED. Each bit represents the result of internally programmed protection logic, automation logic, and status inputs or is mapped directly to a control output. This protocol is also capable of sending up to seven analog values between IEDs. All transmit MIRRORED BITS (TMBs) are processed during each IED processing interval. The status of each TMB is reflected in every transmitted message. When the message is received by the remote IED, received MIRRORED BITS (RMBs) are treated as logic inputs. Messages are transmitted and received asynchronously at rates of up to 38400 bps. MIRRORED BITS communications is used over several communications mediums, including dedicated optical fiber, multiplex digital networks, and analog microwave.

The receiving IED checks each received message in several ways to ensure data reliability. These validations include checks for the following:

- Parity, framing, and overrun errors.
- Multimessage redundancy. Each message repeats the payload multiple times and verifies that each instance is identical and therefore not corrupted by the communications system before the payload is passed into the receiving IED for use as logic inputs.

- Transmit and receive identifiers (IDs). Each peer-to-peer association is set up as a pair with transmit and receive IDs to make sure the MIRRORED BITS communications connections are not inadvertently miscabled in the field.
- Messages received prior to time-out.

If an RMB message passes all of the reliability checks for at least two consecutive good messages, the receiving IED asserts a valid communications status. Multiple paired sessions, or nonpaired unidirectional sessions, are created over multiple individual point-to-point connections.

VI. IEC 61850 GOOSE COMMUNICATIONS

Peer-to-peer messaging within the IEC 61850 communications standard is accomplished with two similarly compliant protocols that differ slightly. These two protocols, IEC 61850 GOOSE and Generic Substation State Event (GSSE), are collectively referred to as Generic Substation Event (GSE). In 2001, GSSE (also known as UCA GOOSE protocol) communication over Ethernet was demonstrated to be interoperable between relays from two different manufacturers. Note that UCA GOOSE protocol is another name for IEC 61850 GSSE and is not to be confused with GOOSE. UCA GOOSE/IEC 61850 GSSE and GOOSE are different protocols that coexist on Ethernet networks, but an IEC 61850 GSSE session in one IED does not communicate with a GOOSE session on another IED. Most contemporary applications use IEC 61850 GOOSE exclusively.

VII. ETHERCAT COMMUNICATIONS

As with most Ethernet protocols, IEC 61850 GOOSE requires that each device sends and/or receives a complete Ethernet frame for every message. The result, even when using multicast messages, is that a large percentage of the network bandwidth is consumed by message administrative information. Therefore, each data source must use a unique message containing pre-engineered network navigation logistics and requiring separate message encoding and decoding. These include unique and well-designed virtual local-area network (VLAN) tags, multicast addresses, maximum delay timers, and GOOSE application IDs.

By contrast, the EtherCAT protocol is a fieldbus protocol that was specifically designed to incorporate data from many EtherCAT nodes into a single message. The telegram can be as large as 4 gigabytes when the message is composed of several Ethernet frames concatenated together. Individual devices are configured to read and write data from specific regions of the telegram, which means that the telegram mapping sequence does not require individual messages for each node. Further, processing of the EtherCAT telegram is similar to an internal IED data bus that directly transfers data from I/O nodes without encoding and decoding messages.

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. This process entails the EtherCAT master executing an application that starts the EtherCAT messages on a fixed interval and evaluates the return. Fig. 7 illustrates an IED acting as an EtherCAT master receiving data from remote I/O devices at fixed locations within the EtherCAT telegram.

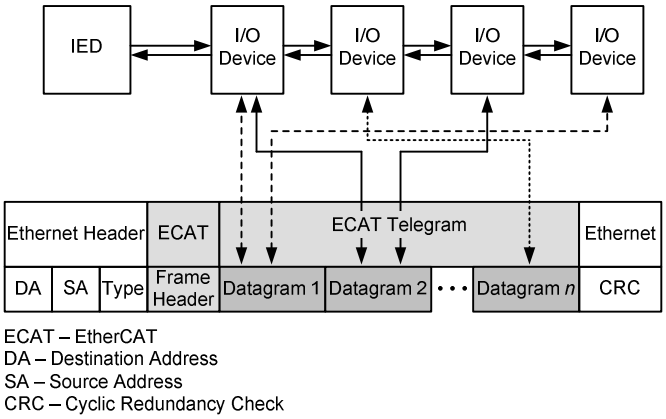

Fig. 7. Network location independent from EtherCAT mapping

VIII. TELEPROTECTION MESSAGE SIZE COMPARISON

Most wide-area teleprotection, telecontrol, or automation schemes typically require the frequent exchange of eight or fewer status points.

The inherent MIRRORED BITS communications message security is useful to minimize the risk of an IED accepting a corrupted message. However, in point-to-point applications, the more important and often overlooked measure is dependability—knowing that the correct data and messages get through when necessary. Message overhead complexity, as a result of message flexibility, and message size are both inversely proportional to the ability to send and parse an uncorrupted peer-to-peer message. The MIRRORED BITS communications message, due to its concise design and transfer, is 4 bytes in length. The IEDs evaluated for this paper support three simultaneous MIRRORED BITS communications connections and therefore transfer a total of 24 Boolean values or combinations of Boolean values, analog values, and engineering access text.

GOOSE messages vary in size based on their flexible payload. However, a GOOSE message requires roughly 157 bytes to transfer eight Boolean values, which is 40 times larger than a MIRRORED BITS communications message.

Unlike IEC 61850 GOOSE messages, EtherCAT messages do not share the bandwidth of an Ethernet network but rather travel over a network dedicated to data acquisition. Therefore, the message overhead is minimized and dedicated to data acquisition rather than GOOSE shared bandwidth Ethernet network navigation settings, such as a VLAN, multicast media access control (MAC) filtering, application IDs, and message configuration naming conventions. In order to transfer eight Boolean values from a single I/O source, EtherCAT communication requires a message of 64 bytes. A message

transferring the maximum possible payload from six interconnected remote nodes is 200 bytes.

These three protocols are contrasted so that the one that best fits the application can be chosen. Assume for time-critical applications that message publication is 3 milliseconds for MIRRORED BITS communications and GOOSE and 1 millisecond for EtherCAT. The required bandwidth is the product of quantity of messages per second and the quantity of bits per message. Table I shows the comparison of these protocols.

TABLE I
COMPARISON OF PROTOCOL THROUGHPUT

Description	MIRRORED BITS Communications	GOOSE	EtherCAT
Size of 8-bit teleprotection message	4 bytes	157 bytes	64 bytes
Required bandwidth for teleprotection message	10656 bits per second	Up to 418248 bits per second	536000 bits per second
Maximum status payload	8 statuses	463 statuses	1,296 statuses
Message size with maximum payload	4 bytes	1,522 bytes	200 bytes
Required bandwidth for maximum payload message	10656 bits per second	Up to 3044000 bits per second	12064000 bits per second

The engineered, purpose-built protocols, MIRRORED BITS communications and EtherCAT, both publish messages as quickly as possible, whether data are changing or not. This guarantees deterministic transfer of information and immediate detection of link failure. The protocols use dedicated actual private networks (APNs) built as dedicated cables in a LAN or provisioned time-division multiplexing (TDM) connections over a WAN—neither of which shares bandwidth. Without the need for message navigation configuration information, the message overhead of both of these engineered protocols is very small and the payload is maximized. The low message overhead creates the most efficient use of bandwidth when connections are provisioned to match the required communications bandwidth.

MIRRORED BITS communications messages are designed to be precisely and constantly the same concise size, repeat the payload for security, and use the same small bandwidth. If the amount of provisioned bandwidth is more than required, the spare bandwidth remains unused.

EtherCAT messages are designed to constantly use the full frame size, support a wide range of payload sizes, and precisely use the entire large bandwidth required.

GOOSE message publication rates change to be more frequent as data change. This means nondeterministic transfer of information and possible delays in detection of link failure. GOOSE messages use dedicated VLANs via unique Ethernet message types and Ethernet frame navigation information on a LAN. They also require provisioned TDM connections over a WAN. Because of message navigation configuration information, the message overhead is larger than that of engineered protocols, which reduces the available frame allocation for payload. This larger message overhead creates inefficient use of bandwidth when connections are provisioned to match the required communications bandwidth. However, the message navigation parameters allow other message types to use spare bandwidth within the shared bandwidth connections and improve efficiency.

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 and interoperability.

IX. WIDE-AREA COMMUNICATIONS DATA TRANSFER SPEEDS

Testing was performed on all three messaging technologies in local- and wide-area distance scenarios. Local messaging was performed using direct serial or Ethernet connections and a small switched Ethernet network. Wide-area connections were tested by transferring those same connections over a synchronous optical network (SONET) connection between mission-critical communications devices.

Fig. 8 illustrates the configuration used for time testing with all protocols. The multiplexer chosen is actually a mission-critical optical network device that has serial and Ethernet local connections and SONET transport for the long-distance fiber link. It transports the serial MIRRORED BITS communications, shared Ethernet GOOSE, and Ethernet EtherCAT over separate time-division allocated segments.

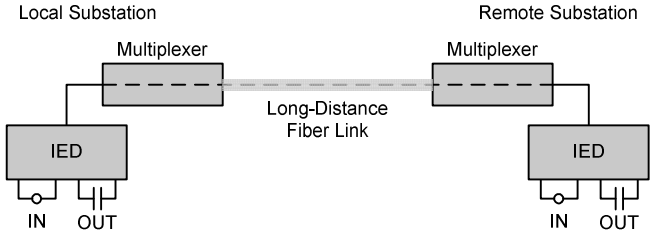

Fig. 8. Test setup

In order to overcome the LAN multicast behavior of GOOSE and use it over a WAN connection, this multiplexer creates a virtual private network (VPN) between stations. Rather than the shared bandwidth network behavior of GOOSE, both MIRRORED BITS communications and EtherCAT protocols use physically segregated networks. This multiplexer builds an APN connection between stations.

For each application, the use of this mission-critical SONET added negligible latency to the messaging between devices. In other words, this technology transports WAN digital messaging between stations so quickly and deterministically that it behaves the same as LAN connections do. The only delay is from the propagation delay of light

through fiber at 5 microseconds per kilometer or 8 microseconds per mile.

Testing has proven that EtherCAT provides a high-speed and deterministic communications method for mission-critical information transfer. It has been demonstrated to reduce the data transmission time from 2 to 3 milliseconds for high-performance IEC 61850 GOOSE messages down to 0.5 milliseconds for EtherCAT. Also, the simpler message processing reduces the transfer time, which includes decoding and using the message contents. As shown in Fig. 9, timing results demonstrate that by removing the protocol encoding and decoding on each transmission of the message, EtherCAT improves performance by 2 milliseconds over similar IEC 61850 GOOSE communications systems, from 3 milliseconds on average using high-performance IEC 61850 GOOSE down to 1 millisecond on average using EtherCAT. This is a 300 percent improvement in transfer time.

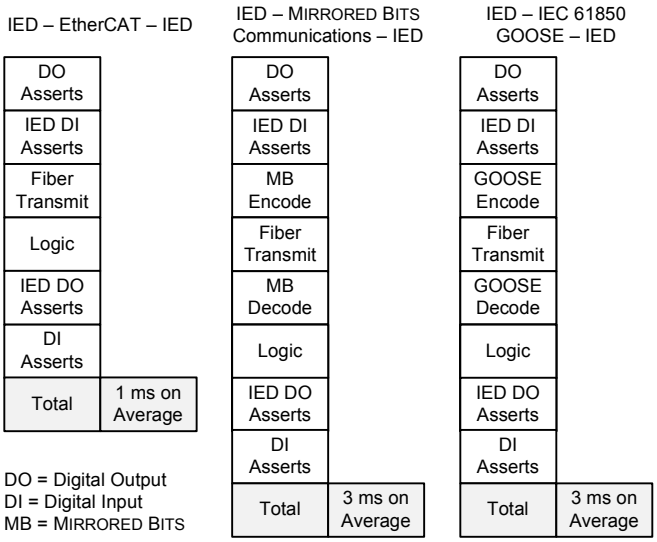

Fig. 9. Communications process and timing results for one-eighth-cycle IED

X. TELEPROTECTION MESSAGE GOODPUT COMPARISON

Goodput is the amount of useful data, user data, or payload that can be processed by, passed through, or otherwise put through a system and received at the correct destination address. For MIRRORED BITS communications and EtherCAT working over private networks, it is simply the measure of application information throughput, the calculation of message payload information exchanged between devices, as opposed to traditional communications message throughput. Goodput as a function of time is a ratio of the delivered amount of application information and the total delivery time. Goodput as a function of message overhead is a ratio of the delivered amount of application information and any packet headers or other overhead. Goodput in a shared network is difficult to know because the network may deliver unwanted messages in addition to the wanted application messages. For the purpose of this message comparison, we do not account for true network behavior, which may include delivery of unwanted and unneeded messages and may experience reconfiguration, congestion, or retransmission of messages. For Ethernet IEC 61850 GOOSE goodput calculations, we assume that they are multicast over a private Ethernet network. Also, it is not possible to measure the actual communications channel message delivery time. Instead, we use the transmission time to compare the three methods. Therefore, we approximate goodput over time (GPT) as follows:

$$\text{GPT} = (\text{payload})/(\text{transmission time}) \quad (1)$$

where:

The payload size is 8 bits for the typical teleprotection application.

We calculate goodput as a function of message size (GPM) as follows:

$$\text{GPM} = (\text{payload})/(\text{total message size}) \quad (2)$$

GPT and GPM for a typical 1-byte teleprotection message, as well as for a message with the maximum possible payload, are compared in Table II.

TABLE II
COMPARISON OF PROTOCOL GOODPUT

Description	MIRRORED BITS Communications	GOOSE	EtherCAT
Size of 8-bit teleprotection message	4 bytes	157 bytes	64 bytes
GPT for teleprotection message	333 bytes per second	333 bytes per second	1,000 bytes per second
GPM for teleprotection message	25%	0.6%	1.6%
Maximum status payload	8 statuses	463 statuses	1,296 statuses
Message size with maximum payload	4 bytes	1,522 bytes	200 bytes
GPT for message with maximum payload	333 bytes per second	19.3 kilobytes per second	162 kilobytes per second
GPM for message with maximum payload	25%	3.8%	81%

XI. DIGITAL MESSAGES HAVE MEASURABLE SECURITY AND DEPENDABILITY REQUIREMENTS

IT, OT, protection, automation, and communications engineers must collaborate to understand all of the design criteria affecting PCM communications and applications. Dependability and security to deliver every message uncorrupted every time are specifically essential for telecontrol, teleprotection, interlocking, and high-speed automation. The required performance of OT networks may not be well understood by some Ethernet network designers, but it is well documented. IEC 60834-1 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.

Ethernet technology permits simple LAN assembly and sophisticated failure recovery mechanisms. However, by its design, it is impossible to create Ethernet networks with 100 percent dependability and security. Also, substandard performance is not easily detected, so when Ethernet is used in mission-critical applications, it is especially important that the degradation be identified, measured, and improved. And although Ethernet will never reach the security and dependability of direct peer-to-peer connections, such as with MIRRORED BITS communications, it is the responsibility of the communications designer to use every tool and method available to drive out as much risk of dropped packets and potential catastrophic failures as possible. Shared networks must be designed to satisfy the performance requirements of the most critical digital messaging on the network, such as peer-to-peer teleprotection and interlocking. The other messaging will enjoy greater security and dependability than it may need today. However, the availability of the better message performance encourages innovation and improvements in these other applications as well. In digital systems, both continuous and impulsive disturbances can occur.

Regardless of the type of communications channel used, poor installation and environmental issues may introduce noise. In fact, it is easier to isolate direct serial and Ethernet connections from noise than a larger switched Ethernet network, but for the content of this paper, we assume that noise could equally affect channels carrying MIRRORED BITS communications, IEC 61850 GOOSE, or EtherCAT. Also, because MIRRORED BITS communications and EtherCAT traverse separate private direct links, there is no opportunity for congestion or reconfiguration that results in dropped packets or unexpected devices or network configuration that results in extra messaging. They do not offer the flexibility of multiplexing other communications; this is intentional to maximize speed but also dependability and security of message delivery.

Either noise or, in the case of a shared Ethernet network, delivery of unwanted messages adversely affects delivery of appropriate 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 legitimate command messages, reducing dependability.

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 [8]. 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 a 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 a device receiving an unwanted command P_{uc} to be approximated as follows:

$$P_{uc} \approx \frac{N_{uc}}{N_B} \tag{3}$$

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:

$$P_{um} = \frac{N_{umr}}{N_{umt}} \tag{4}$$

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:

$$P_{mc} \approx \frac{N_T - N_R}{N_T} \tag{5}$$

where:

N_T is the number of commands transmitted.

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:

$$P_{mm} = \frac{\left(N_{tm} - N_{wmr}\right)}{N_{tm}} \quad (6)$$

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 III 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 III
PERFORMANCE GUIDANCE FIGURES FOR VARIOUS TELEPROTECTION SCHEMES

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

If designers do not fully understand the environmental factors that can impact their decisions and translate that knowledge into an understanding of the consequences, they are simply not performing adequate due diligence design. When using MIRRORED BITS communications, IEC 61850 GOOSE, or EtherCAT, the associated private serial channel, shared Ethernet, or private Ethernet network must be designed and tested to meet security and dependability of message delivery.

The IEC 60834-1 standard assumes dedicated channels for teleprotection, interlocking, and high-speed automation, and so the performance guidelines do not address shared networks, such as Ethernet. Therefore, probability of receipt of unwanted messages and probability of missed messages are not yet addressed. However, they are necessary measures of network behavior and performance for comparison of multiple designs for reliability.

XII. CONCLUSION

Testing has proven that EtherCAT provides a high-speed and deterministic communications method for mission-critical information transfer. It has been demonstrated to reduce the data transmission time from 2 to 3 milliseconds for high-performance IEC 61850 GOOSE messages down to 0.5 milliseconds for EtherCAT. Also, the simpler message processing reduces the transfer time, which includes decoding and using the message contents, from 3 milliseconds on average using high-performance IEC 61850 GOOSE down to 1 millisecond on average using EtherCAT. This is a 300 percent improvement in transfer time.

Although the breaker failure initiate (the time required to send an initiate signal from the primary protective relay to the breaker failure relay) is impacted by the improvement in transfer time, it is also affected by other factors. However, the duration of the distribution of the breaker failure trip (the time to send breaker failure tripping signals to local and remote circuit breakers) essentially becomes the transfer time if the relays use high-speed output contacts that operate in microseconds. Therefore, the mission-critical trip function is improved by 300 percent by changing the transfer time from 3 milliseconds to 1 millisecond. This, in turn, reduces the wear on the power system apparatus by reducing the duration of operation under fault conditions by 300 percent.

In the example of improving traditional breaker failure clearing times with faster communication, rather than the expensive and time-consuming prospect of replacing circuit breakers, EtherCAT not only minimizes damage due to breaker failure events but also maintains system stability. This new deterministic messaging not only improves traditional protection and control schemes but also allows designers to envision strategies that were not previously possible. New EtherCAT high-speed and deterministic data acquisition behavior over long distances will support creative designs unconstrained by previously typical communications latencies.

The major benefit EtherCAT offers is that the time required to create and verify the message is reduced. The time on the wire is governed by the laws of physics and is independent of the communications mediums used.

MIRRORED BITS communications is the most efficient method of delivering useful data per message size for a teleprotection payload. For typical teleprotection messages, MIRRORED BITS communications is not only more efficient but also as fast as GOOSE. EtherCAT is faster than both. However, both GOOSE and EtherCAT have the flexibility to communicate with multiple devices and can send larger payloads for different applications. For larger payloads, EtherCAT delivers much more useful data per message size than either MIRRORED BITS communications or GOOSE.

Another important consideration is that these digital communications schemes simplify trip functions by eliminating physical components, such as breaker failure initiate output contacts to communicate breaker failure over copper conductors, as well as lockout relays. When either of these physical components fail, power system apparatus are damaged or destroyed. Complicated physical protection schemes can also cause delays in determining root cause, assessing damage, and re-energization after a fault. Correctly engineered, tested, and commissioned interlock and teleprotection done via digital messaging via MIRRORED BITS communications, IEC 61850 GOOSE, or EtherCAT provide higher reliability and security of protection functions.

IEC 60834-1 describes requirements for message propagation time and guidelines for communications channel reliability. Message propagation time through the communications channel must be under 3 milliseconds for teleprotection, interlocking, and high-speed automation applications. Also, unwanted messages delivered to the teleprotection receiver may delay processing or, worse, push a wanted message off an input queue or buffer so that it is never processed.

Probability of receipt of unwanted messages and probability of missed messages are new concerns for these applications brought about by the use of shared Ethernet networks. They are necessary measures of network performance, security, dependability, and reliability.

XIII. REFERENCES

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

[2] M. Gugerty, R. Jenkins, and D. 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.

[3] I. Stevens, N. Fischer, and B. Kasztenny, "Performance Issues With Directional Comparison Blocking Schemes," proceedings of the 36th Annual Western Protective Relay Conference, Spokane, WA, October 2009.

[4] E. Atienza and R. Moxley, "Improving Breaker Failure Clearing Times," proceedings of the 36th Annual Western Protective Relay Conference, Spokane, WA, October 2009.

[5] IEEE Standard C57.109-1993, IEEE Guide for Liquid-Immersed Transformers Through-Fault-Current Duration, 1993.

[6] 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.

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

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

XIV. BIOGRAPHIES

David Dolezilek received his BSEE from Montana State University and is the technology director of 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 global standardization and security of communications networks and systems in substations.

Normann Fischer received a Higher Diploma in Technology, with honors, from Witwatersrand Technikon, Johannesburg, in 1988, a BSEE, with honors, from the University of Cape Town in 1993, and an MSEE from the University of Idaho in 2005. He joined Eskom as a protection technician in 1984 and was a senior design engineer in the Eskom protection design department for three years. Normann then joined IST Energy as a senior design engineer in 1996. In 1999, he joined Schweitzer Engineering Laboratories, Inc. as a power engineer in the research and development division. Normann was a registered professional engineer in South Africa and a member of the South Africa Institute of Electrical Engineers. He is currently a member of IEEE and ASEE.

Robert Schloss is a lead automation engineer in the automation and integration engineering division of Schweitzer Engineering Laboratories, Inc. (SEL). He received his BSEE from the University of Idaho and has been with SEL since 2004. His experience includes research and development product engineering, as well as system design and commissioning of large-scale power system automation projects for critical assets. He is currently a member of IEEE.