Case Study: Dramatic Improvements in Teleprotection and Telecontrol Capabilities Via Synchronous Wide-Area Data Acquisition

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

Presented at the
2nd Annual Protection, Automation and Control World Conference
Dublin, Ireland
June 27–30, 2011

Case Study: Dramatic Improvements in Teleprotection and Telecontrol Capabilities Via Synchronous Wide-Area Data Acquisition

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

***Abstract*—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. The resulting measured values are used by local protection algorithms executed in the IED main processor subsystem each time data are retrieved from the IED data acquisition subsystem. If abnormal conditions exist, relays record information, make decisions, and take action. In addition to detecting faults and tripping circuit breakers, the IED communications processor subsystem creates and publishes digitized messages. These messages communicate measured values from one IED to another over short or long communications links. This same communications processor subsystem also receives messages containing measured values from other IEDs and passes them to the IED main processor subsystem. By reprocessing these measured values from 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, defined as protection over a distance, includes algorithms that rely on receiving measured values from other locations too distant to be directly wired to the IED, including 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, defined as control over a distance, includes 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.

Teleprotection and telecontrol require that the messages travel from point to point with a high degree of security and dependability. Communications techniques to ensure secure and dependable transfer of measured values add message overhead and therefore additional processing latency within both the sending and receiving IED communications processor subsystems. The type and distance of the communication also determine the latency in message transit. Therefore, the available type, accuracy, and speed of remote decision-making methods are bounded by the time to create, publish, transfer, receive, verify, and parse messages that contain measured values.

This paper compares the improved performance of remote decisions and investigates the opportunity for new algorithms by communicating the raw values from direct-wired instrument transformers and the status of contact inputs over great distances. Creative use of a deterministic Ethernet fieldbus protocol over a deterministic wide-area Ethernet communications infrastructure creates wide-area synchronous raw data publication for use as direct inputs to remote IED data acquisition subsystems. This eliminates the processing burden and latency associated with the creation, publication, transfer, reception, verification, and parsing of messages between IED communications processor subsystems.

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. 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 media. 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.

II. Digital Messaging

It is important to note that data received via digital messaging were actually measured or calculated in the 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.

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, 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, and DNP3, each managed by an SDO and/or users group committee funded by a collection of manufactures 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 that 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.

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 [1]. The designer must guarantee that each of the following high-priority tasks happens each processing interval within an IED:

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

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 protection, control, and monitoring applications. Then they are standardized and offered via a "reasonable and nondiscriminatory" license by the SRO to facilitate data exchange among multiple manufacturers.

III. 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.

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. 1 by $t = t_a + t_b + t_c$ [2]. 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.

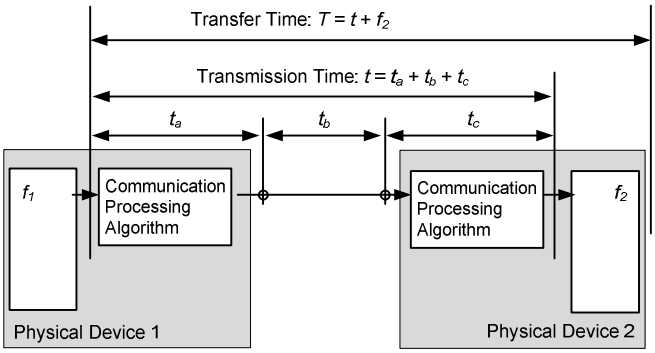

Fig. 1. Transmission time definition

The two most prevalent message technologies in use in the electric power industry today are MIRRORED BITS communications and IEC 61850 Generic Object-Oriented Substation Event (GOOSE).

IV. 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 media, 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.

V. MIRRORED BITS COMMUNICATIONS DATA TRANSFER SPEED

MIRRORED BITS communications messages are published and received every processing interval of the central processing unit (CPU) in an IED. For this paper, we consider specific IEDs that have a concise high-speed MIRRORED BITS communications message that transfers eight Boolean values. As with all protocols, other payload sizes can be implemented. The time latency to move the payload of eight Boolean values includes the time to detect and communicate the change of information to the second IED (transmission time) plus the time to process the message in the receiving IED (processing interval) for an aggregate transfer time (transmission time plus the processing interval of the second IED). For this paper, we consider IEDs that operate every one-eighth of a power system cycle (every 2 milliseconds) or every one-quarter of a cycle (every 4 milliseconds) for a 60 Hz system. The associated transfer speeds for specific IEDs local to one another using MIRRORED BITS communications over a short cable connection are as follows:

- Operating every one-eighth of a cycle on a 60 Hz system:
  - Typical transmission time is 2 to 3 milliseconds.
  - Typical transfer time is 3 to 4 milliseconds.
- Operating every one-quarter of a cycle on a 60 Hz system:
  - Typical transmission time is 3 to 5 milliseconds.
  - Typical transfer time is 4 to 6 milliseconds.

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. IEC 61850 GOOSE Communications Data Transfer Speed

An important difference with IEC 61850 GOOSE messages is that once published, they are received in the subscriber IEDs within one processing interval only if the Ethernet network correctly delivers them to the IEDs. This relies heavily on the network design and the configuration of the Ethernet switches. The shared bandwidth methods of Ethernet do not provide deterministic behavior of GOOSE. However, very careful design of message logistics in the IEDs and switches, restriction of Ethernet traffic, and use of best practice network design can make tightly controlled Ethernet networks behave more deterministically. Mirrored Bits communications travels over direct serial cables or tunneled Ethernet connections that travel point to point rather than the multicast behavior of IEC 61850 GOOSE messages. Mirrored Bits communications maps dedicated IED logic bits (TMBs) into outgoing messages, and the receiving IEDs map the contents to dedicated IED logic bits (RMBs). Transmit and receive GOOSE message contents are not predetermined, and manufacturers are free to choose from many types of IED data. The time latency to move the GOOSE payload includes the time to detect and communicate the change of information to the second IED (transmission time) plus the time to process the message in the receiving IED (processing interval) for an aggregate transfer time (transmission time plus the processing interval of the second IED). The GOOSE payload size is restricted by the Ethernet technology, not by consideration of the applications it serves. Therefore, the GOOSE message can be as large as a single Ethernet frame and transfer hundreds of Boolean values within its payload. Most applications require the exchange of less than eight Boolean values, even though the IEDs support the exchange of a payload size up to the full Ethernet frame. However, this also means that even messages with small payloads require the full Ethernet frame components, including source address, destination address, network logistics, and error checks.

The protocol overhead of GOOSE messages is very large and requires significant processing by the sending and receiving IEDs. Great care must be exercised by IED designers to make sure that the messages are processed quickly. The overhead of a single GOOSE message is 123 bytes. Based on IEC 61850 methods, each Boolean value requires 3 bytes for encoding, which also causes more payload message overhead. Therefore, great care must be exercised by those configuring GOOSE messages to make sure that the payloads are as small as possible to ensure that the messages are processed as quickly as possible.

For this paper, we consider the same IEDs that support Mirrored Bits communications and operate every one-eighth of a power system cycle (every 2 milliseconds) or every one-quarter of a cycle (every 4 milliseconds) for a 60 Hz system. The associated transfer speeds for the specific IEDs local to one another over a short cable connection or through a single correctly configured Ethernet switch using IEC 61850 GOOSE messages are as follows:

- Operating every one-eighth of a cycle on a 60 Hz system:
  - Typical transmission time is 2 to 3 milliseconds.
  - Typical transfer time is 3 to 4 milliseconds.
- Operating every one-quarter of a cycle on a 60 Hz system:
  - Typical transmission time is 3 to 5 milliseconds.
  - Typical transfer time is 5 to 6 milliseconds.

GOOSE messages serve several different applications, and each application can have different performance requirements. IEC 61850 classifies application types based on how fast the messages are required to be transmitted among networked IEDs [3]. The standard also specifies the performance of each type of application, documented as the time duration of message transmission. Table I lists the message types.

TABLE I
IEC 61850 Message Types and Performances

Type	Application	Performance Class	Requirement (Transmission Time)
1A	Fast Messages (Trip)	P1	10 ms
		P2/P3	3 ms
1B	Fast Messages (Other)	P1	100 ms
		P2/P3	20 ms
2	Medium Speed		100 ms
3	Low Speed		500 ms
4	Raw Data	P1	10 ms
		P2/P3	3 ms
5	File Transfer		≥1000 ms
6	Time Synchronization		(Accuracy)

VIII. 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 Ethernet nodes into a single message. The telegram can be as large as 4 gigabytes when the message is comprised 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. 2 illustrates an IED acting as an EtherCAT master receiving data from remote I/O devices at fixed locations within the EtherCAT telegram.

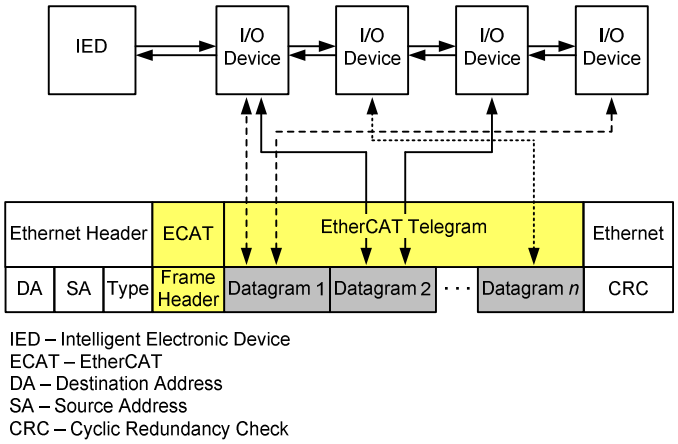

Fig. 2. Network location independent from EtherCAT mapping

IX. EtherCAT Communications Data Transfer Speed

In order to achieve the needed network speed for critical applications, EtherCAT devices use a low-level, on-the-fly processing method where all devices within a network segment receive the entire EtherCAT message [4].

Because an EtherCAT frame comprises the data of many devices in send and receive directions, the usable data rate increases to more than 90 percent. This means that the connection works best on a dedicated network where EtherCAT can use the entire bandwidth. EtherCAT works on a switched network, but the performance degrades. This paper examines a dedicated network connection for EtherCAT. The behavior of EtherCAT messages on a dedicated network eliminates the time delay and processing burden of message encoding and decoding processes between the detection of an input change of state and the subsequent update of that value in a decision-making process in a remote IED. For teleprotection, an EtherCAT telegram comprised of a single Ethernet frame is sufficient. This single-frame message is the smallest EtherCAT telegram possible, is 1,500 bytes in size, and is capable of transferring 1,296 statuses.

For this paper, we consider the same IEDs that support Mirrored Bits communications, IEC 61850 GOOSE messages, and EtherCAT and operate every one-eighth of a power system cycle (every 2 milliseconds) for a 60 Hz system. The associated transfer speeds for the specific IEDs local to one another on an EtherCAT network are as follows:

- Operating every one-eighth of a cycle on a 60 Hz system
  - Typical transmission time is 1 to 2 milliseconds.
  - Typical transfer time is 3 to 4 milliseconds.
- Operating every one-quarter of a cycle on a 60 Hz system
  - Typical transmission time is 1 to 2 milliseconds.
  - Typical transfer time is 5 to 6 milliseconds.

X. 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 1,500 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 4 milliseconds for Mirrored Bits communications and GOOSE, and

EtherCAT runs as fast as the connection allows. Table II shows the comparison of these protocols.

TABLE II
COMPARISON OF PROTOCOLS

Description	MIRRORED BITS Communications	GOOSE	EtherCAT
Size of 8 bit teleprotection message	4 bytes	157 bytes	1,500 bytes
Required bandwidth for teleprotection message	4000 bps	Up to 314000 bps	48000000 bps
Maximum status payload	8 statuses	463 statuses	1,296 statuses
Message size with maximum payload	4 bytes	1,522 bytes	1,500 bytes
Required bandwidth for maximum payload message	4000 bps	Up to 3044000 bps	48000000 bps

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 the 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.

XI. WIDE-AREA DATA 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. 3 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.

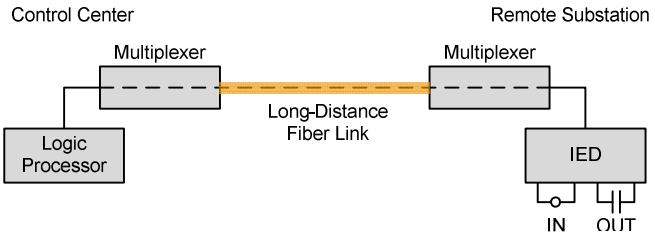

Fig. 3. Test setup

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 synchronous optical network added no measurable 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.

XII. BENEFITS OF HIGH-SPEED COMMUNICATION AS APPLIED TO PROTECTION SYSTEMS

The benefit that communications schemes afford to protection systems is that they can 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.

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. 4. 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.

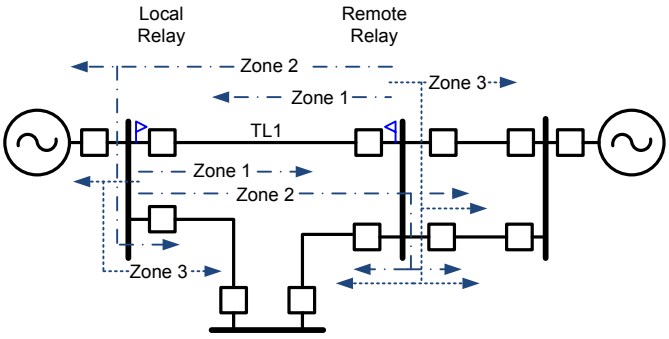

Fig. 4. Sketch of a simple power system with zone reaches superimposed

In Fig. 4, 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. 4 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. So 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 a permission signal from the remote ends [5]. 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. 5 illustrates the basic operating principle of a permissive overreaching transfer trip (POTT) scheme.

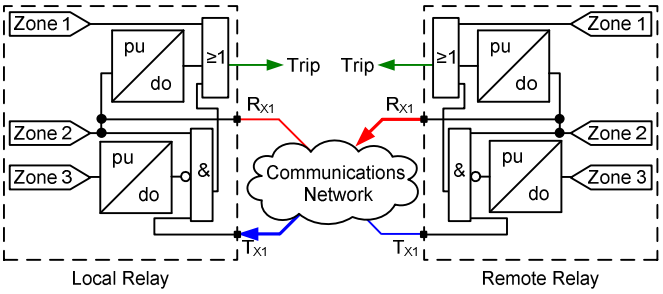

Fig. 5. Simple sketch of a POTT scheme

Fig. 6 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.

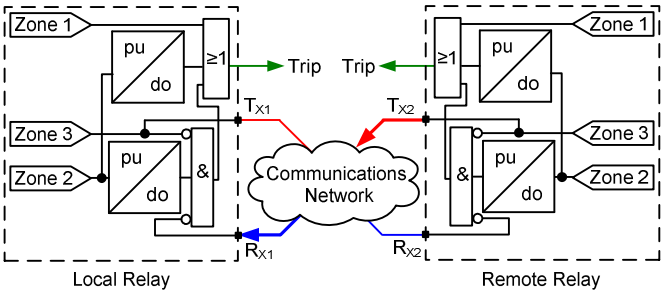

Fig. 6. Simple sketch of a DCB scheme

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. 7 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).

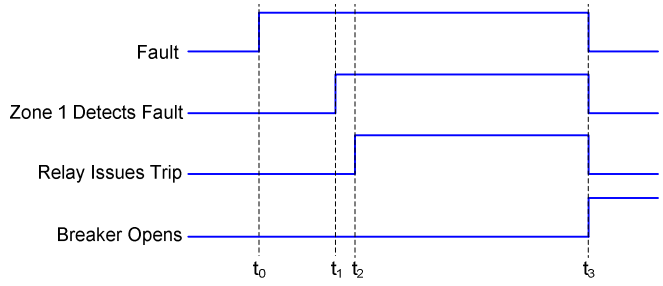

Fig. 7. Timing diagram for a fault within the Zone 1 reach

Fig. 8 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.

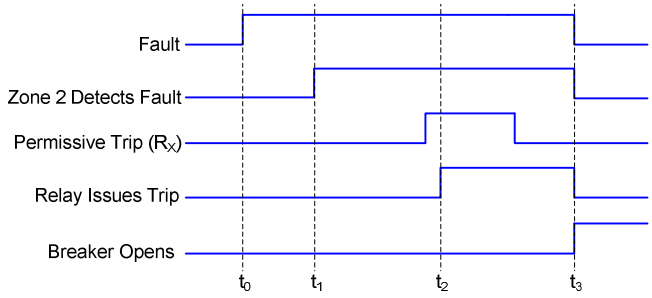

Fig. 8. Timing diagram for a fault outside of the Zone 1 reach

Protection engineers strive to have the timing diagram shown in Fig. 8 closely resemble the timing diagram shown in Fig. 7. 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 [6]. 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 (above) 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.

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 [7]. 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.

XIII. Summary

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 minimizes damage due to breaker failure events and maintains system stability. This new deterministic messaging not only improves traditional protection and control schemes but also allows designers to envision strategies that were previously not 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 media used.

XIV. References

[1] 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.

[2] 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.

[3] IEC 61850 Standard. Available: http://www.iec.ch.

[4] M. Rourke, D. Dolezilek, and F. Chumbiauca, "Application of Ethernet Fieldbus to Substation RTU and Automation Networks," proceedings of the 13th Annual Western Power Delivery Automation Conference, Spokane, WA, March 2011.

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

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

[7] IEEE C57.109-1993, Guide for Liquid-Immersed Transformers Through-Fault-Current Duration. Available: http://standards.ieee.org.

XV. 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 protection design department at Eskom for 3 years. He 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 an automation engineer in the research and development automation and integration division at Schweitzer Engineering Laboratories, Inc. (SEL), serving as the product engineer for programmable automation products. His previous experience includes 6 years in SEL engineering services as an automation engineer on power system automation projects (specifically with remedial action schemes, load shedding, voltage control, generation control, and SCADA). He received his BSEE from the University of Idaho and has been with SEL since 2004.