Case Study: New Testing and Verification Practices for Virtual Wiring Among IEDs Via Ethernet Communications

Timothy Tibbals and David Dolezilek
Schweitzer Engineering Laboratories, Inc.

Presented at the
Southern African Power System Protection Conference
Johannesburg, South Africa
November 10–12, 2010

Previous revised edition released July 2010

Originally presented at the
1st Annual Protection, Automation and Control World Conference, June 2010

Case Study: New Testing and Verification Practices for Virtual Wiring Among IEDs Via Ethernet Communications

Timothy Tibbals and David Dolezilek, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—The use of digital communication, including IEC 61850 Generic Object-Oriented Substation Event (GOOSE), has created opportunities to eliminate hard-wired copper terminations to exchange status values among intelligent electronic devices (IEDs). Routed and nonrouted communications over wireless links and copper or fiber-optic cables greatly reduce the amount of labor and physical wire needed to convey discrete and analog values among IEDs and controllers. This eliminates many opportunities for wiring mistakes before they occur.**

However, replacing hard-wired connections with digital communication requires new engineering practices. The effort needed to convey values among IEDs has migrated with this modernization from the act of making physical terminations to the act of making logical interconnections within the IEDs. Now, instead of or in conjunction with traditional hard-wiring, values within IEDs are virtually wired to other IEDs via digital communication. IED values are published as contents of digital communications messages, and other IEDs subscribe to these messages. The message contents are then virtually wired to logical terminations within the receiving IED.

Exchange via nonrouted digital communication remains very fast, deterministic, and automatically connected to predefined logical terminations within the publisher and subscriber. This method requires no termination configuration, so there is no room for error. However, newer intranet multicast methods, such as IEC 61850 GOOSE, offer more flexibility and function over a routable Ethernet network. GOOSE exchange among IEDs requires logical termination configuration at both the publishing and subscribing IEDs. Therefore, confirmation that this was completed correctly needs to occur during the testing and commissioning of systems.

Global experience demonstrates that over 50 percent of copper terminations, associated cost and labor, and opportunities for mistakes are eliminated via the use of digital communication among peer IEDs. However, end users have questions, such as: How do test technicians selectively block signals communicating over Ethernet without interrupting all relay communication?

This paper discusses the methods developed to document and test the virtual wiring, which replaces traditional wiring drawings and end-to-end continuity testing.

Discussion of the evolution of best engineering practices based on experiences from numerous installed systems provides valuable insight for testing, commissioning, and maintaining routable Ethernet networks using one or more of the IEC 61850 protocols for peer-to-peer data exchange.

I. Introduction

Substation integration and automation systems today often perform substation data concentration using discrete I/O interface modules, interposing relays, and serial communication to intelligent electronic devices (IEDs) via a direct connection. This information is collected and passed to supervisory control and data acquisition (SCADA), either directly from the data concentrator or after a protocol translation, if needed by the SCADA master.

Rather than propagate the existing direct-connect I/O designs, new alternatives incorporate the existing IEDs and improve the integration and automation, while also simplifying the system architecture. These designs achieve not only simplification of the installation but significant reduction in copper wiring. The National Institute of Standards and Technology approves protocol standards created by a standards-related organization (SRO) and offered via a "reasonable and nondiscriminatory" license, including proprietary protocols. Field-proven designs have used serial SRO protocols successfully for years. Newer designs also use several protocols within IEC 61850 to support peer-to-peer IED communication, human-machine interfaces (HMIs), and SCADA connections. Fully utilizing the available I/O in the relays and other IEDs via communications connections eliminates unneeded equipment and reduces configuration, installation, commissioning, and maintenance costs [1].

However, this presents a new challenge to those implementing and testing these systems. These new technologies require new tools and concepts to replace the previous, familiar test processes and provide an understanding of the unseen data flow inside the communications network and a certainty that the protection and control systems will operate properly.

II. Communications Design Overview

Prior to Ethernet network-based designs, substation communication was designed with an integration architecture that included a combination of direct-wired I/O modules, transducers, microprocessor-based relays, and other IEDs. A station gateway or data concentrator passed remote controls issued from the remote SCADA master onto the protective relays, which operated the substation apparatus. The station gateway collected breaker statuses, alarms, and other digital inputs. Metering quantities were collected from separate transducers, and relay target statuses were collected directly from the multiple connected relays. The station gateway concentrated the data from the IEDs into a single database and passed data to the remote SCADA console using a protocol

supported by the SCADA master vendor, which could be either a serial or Ethernet connection.

Because this design requires extensive I/O wiring, interposing relays, additional protocol modules, and configuration expertise, alternate designs are developed using the following criteria:

- Reduce the number of programmable devices.
- Reduce I/O wiring.
- Utilize data within existing protective relays.
- Use communication wherever possible to collect SCADA data.
- Apply protective relays to implement local automation.
- Implement fiber-optic network communications systems for HMI, SCADA, and engineering access.
- Provide integrated network communication compatible with the existing online SCADA master.
- Ensure that the integration and automation system is compatible with the two different relay platforms or vendors for dual primary protection.
- Eliminate the standalone Sequential Events Recorder (SER) devices and metering transducers.

These new integration and automation designs rely heavily on the communications infrastructure and the communication of I/O between the relays. Serial designs rely on SRO protocol standards, and Ethernet designs rely on IEC 61850 Generic Object-Oriented Substation Event (GOOSE) for I/O exchange and other Ethernet-based messaging for SCADA and engineering access needs.

III. Implementing New Technology and Methods

A. HMI Development

Most HMI software today provides for Object Linking and Embedding for Process Control (OPC) communications capability. Migrating substation communication to IEC 61850 methods uses Transmission Control Protocol/Internet Protocol-based (TCP/IP-based) Manufacturing Message Specification (MMS) communication over Ethernet to update SCADA and HMI data. TCP/IP supports the required client/server polling and reporting methods for data exchange. There are several off-the-shelf MMS-to-OPC communications drivers available today that can be used with existing HMI software so that present OPC tag databases can be updated with the new IEC 61850 naming conventions. In these systems, the OPC tag names carry the IEC 61850 data name and preserve the data names across the MMS-to-OPC transition.

Using OPC to update the HMI software enables the reuse of existing HMI template views. These templates associate the HMI value fields with an OPC tag rather than an incoming protocol map. OPC is essentially the method by which protocol software and HMI software communicate to one another within the PC.

B. Communications Commissioning and Checkout

One important complication of the technology shift is the increasing portion of the protection system design that resides in algorithms and logic in relays [2]. With the elimination of devices and hard-wired connections, new methods of testing and documentation are needed. Previous substation designs utilized wiring diagrams or drawings for point verification. Points previously hard-wired are now broadcast onto an Ethernet network via IEC 61850 GOOSE messages. For any integrated system, a methodical system checkout must be performed during commissioning to verify proper data flow. The results of this testing and verification must be documented and archived for future review. Using IEC 61850 MMS and GOOSE for the virtual cabling between IEDs in place of physical field cables requires some slightly different documentation, but the digital wiring within the virtual and physical cables requires the same basic wiring and checkout concepts. Each GOOSE message becomes a virtual cable with the message contents virtually wired only to the other IEDs that need the data. No other IEDs receive the data. This is done by creating an IEEE 802.1Q virtual local-area network (VLAN) between the source IED and the destination IEDs.

Fig. 1 shows example output from an IED GOOSE configuration tool that documents the data conveyed via the incoming virtual wires. The source IED, virtual cable name, and data description concatenate together in the entry for the control data item column. The destination IED name is in the IED name column, and the destination IED virtual termination point is described in the control input column. For example, Lines 1 and 2 describe mapping the two status values of the multistate position of Circuit Breaker #1 from the FEEDER_RELAY_1 to virtual bits VB001 and VB002 in the TRANSFORMER_RELAY_1 via Virtual_Cable_A. Line 9 describes mapping the supervisory status of the message quality of Virtual_Cable_C to virtual bit VB009 in the TRANSFORMER_RELAY_1. Also, Lines 11, 12, and 13 describe mapping the three dead-banded floating point values of Phase A, B, and C watts from the AUTO_CONTROLLER_1 to remote analogs RA002, RA003, and RA004 in the TRANSFORMER_RELAY_1 via Virtual_Cable_B. These virtual wiring descriptions can be given in a variety of file formats so that they can be incorporated into a wide variety of existing documentation systems. This information replaces point-to-point wire connections. It is used to facilitate commissioning testing and system troubleshooting.

IED Name	Control Input	Control Data Item
TRANSFORMER_RELAY_1	VB001	FEEDER_RELAY_1.Virtual_Cable_A.PRO.BK1XCBR1.Pos.stVal bit 0
TRANSFORMER_RELAY_1	VB002	FEEDER_RELAY_1.Virtual_Cable_A.PRO.BK1XCBR1.Pos.stVal bit 1
TRANSFORMER_RELAY_1	VB003	FEEDER_RELAY_1.Virtual_Cable_A.PRO.BKR1CSWI1.Pos.stVal bit 0
TRANSFORMER_RELAY_1	VB004	FEEDER_RELAY_1.Virtual_Cable_A.PRO.BKR1CSWI1.Pos.stVal bit 1
TRANSFORMER_RELAY_1	VB005	FEEDER_RELAY_1.Virtual_Cable_A.Message Quality bit 0
TRANSFORMER_RELAY_1	VB006	AUTO_CONTROLLER_1.Virtual_Cable_B.Message Quality bit 0
TRANSFORMER_RELAY_1	VB007	REMOTE_IO_DEVICE_1.Virtual_Cable_C.ANN.SVGGIO1.Ind01.stVal bit 0
TRANSFORMER_RELAY_1	VB008	REMOTE_IO_DEVICE_1.Virtual_Cable_C.ANN.SVGGIO1.Ind02.stVal bit 0
TRANSFORMER_RELAY_1	VB009	REMOTE_IO_DEVICE_1.Virtual_Cable_C.Message Quality bit 0
TRANSFORMER_RELAY_1	RA001	AUTO_CONTROLLER_1.Virtual_Cable_B.MET.METMMXU1.Hz.mag.f
TRANSFORMER_RELAY_1	RA002	AUTO_CONTROLLER_1.Virtual_Cable_B.MET.METMMXU1.W.phsA.mag.f
TRANSFORMER_RELAY_1	RA003	AUTO_CONTROLLER_1.Virtual_Cable_B.MET.METMMXU1.W.phsB.mag.f
TRANSFORMER_RELAY_1	RA004	AUTO_CONTROLLER_1.Virtual_Cable_B.MET.METMMXU1.W.phsC.mag.f

Fig. 1. Configuration tool GOOSE virtual wiring output

In addition to the GOOSE virtual wiring descriptions, the actual configuration files that will be used within the IEDs to be commissioned should be validated. IEC 61850 methods can be used for this purpose. The Substation Configuration Language (SCL) files contain naming and configuration information, which is referenced to verify that each IED has the correct configuration file. Fig. 2 shows a device identification report collected from an IED. It shows the configured IED name (iedName=PAC_SLAVE_C), which is retrieved from the Configured IED Description (CID) file stored in the IED via the vendor IEC 61850 configuration software, as shown in Fig. 3. This check verifies that the correct configuration is in the IED to create the expected GOOSE virtual wiring, which is then verified by the GOOSE virtual wiring descriptions.

```
"FID=PAC-R200-V0-Z002002-D20070810","08CB"
"DEVID=PAC_SLAVE_C","05E0"
"iedName=PAC_SLAVE_C_00","07F8"
"type=PAC","047A"
"configVersion=ICD-PAC-R201-V0-Z002002-D20080108","0D42"
```

Fig. 2. Identification report with IED name

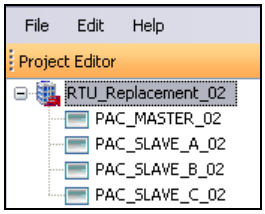

Fig. 3. Configuration software stores IED name

C. Verification of Virtual Peer-to-Peer Channels

More basic communications checks are made using standard Ethernet methods, such as the ping command. A successful ping command executed by a network-connected PC validates the IED connection through the network to the PC and ensures that the IED Ethernet connectivity and some part of the network configuration are correct. However, multicast GOOSE messages are intended to traverse the network between IEDs when in service and only to the PC for testing. Therefore, it is essential to verify that messages from each publishing IED in a virtual wiring connection can traverse the network to each subscribing IED. Some IEDs have implemented the ping command. Fig. 4 shows a screen capture of the ping command from an IED Ethernet interface to verify that it has connectivity to the other IED on the opposite end of its virtual GOOSE wire.

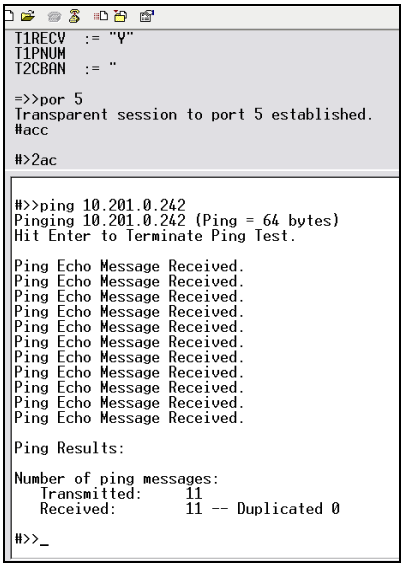

Fig. 4. IED ping command

IV. Changes to Methodology

The major difference that affects all parts of commissioning and testing is that the new integration and automation communications networks connect to Ethernet ports on each IED. The single Ethernet connection uses shared bandwidth methods to merge numerous communications protocols and numerous simultaneous communications channels over that single Ethernet port. It is not clear to the technician what communication is active by looking at the Ethernet cable attached to the IED. It is not evident what virtual cables the IED is publishing via GOOSE, nor is it evident which other IEDs are subscribing. Perhaps most different is that there is no way to segregate communication at the IED level. Once the cable is disconnected, all simultaneous communication on the shared Ethernet media is disabled.

A. Use More Microprocessor-Based IED Multifunction Capabilities

Using functions already built into the microprocessor-based relay is key to being able to eliminate hardware and associated panel wiring. Discrete IEDs for fault detection and breaker failure are replaced with logic and functions already in the microprocessor-based relay. Previous substation designs used microprocessor-based relays for protection only. Other IED functions, such as fault detection and SER recording, were previously performed by standalone dedicated devices. The flexibility and reliability of microprocessor-based relays allow the elimination of dedicated devices because these functions now reside in the relay.

The logic capabilities of IEDs allow various logic schemes that were previously implemented by wiring together the auxiliary relays, timers, and devices to be implemented in a single device using settings [3]. Visualization of these virtual connections and functions as an electrical path maintains the same testing and troubleshooting methods. However, verifying that messages and the data that they transfer are correctly moving over Ethernet requires new, specialized tools. New IED configuration tools use the IEC 61850 methodology of handpicking IED data elements to become a data set, which is published as the virtual wires in the GOOSE virtual cable.

B. Communications Message Testing

Challenges exist when moving the physically connected world to the virtually connected world of digital communication. The verification of these connections requires different tools and methods, although the thought process and verification at the IED basically remains the same.

Because all IED communication is now interleaved through a single Ethernet port, there are different performance classes of traffic and message types being communicated through the same physical connection. When first confirming the correct configuration of the data in a GOOSE message and the connection, compare the GOOSE message being communicated on the Ethernet network to the IED SCL-based configuration file. Fig. 5 shows a screen capture from the Ethernet traffic analyzer, Ethereal®, a freeware software. It shows the decoding of an Ethernet telegram protocol data unit associated with the remote terminal unit (RTU) replacement project illustrated in Fig. 3. Fig. 5 contains a GOOSE message on the left and the configuration software view of the GOOSE message data set on the right.

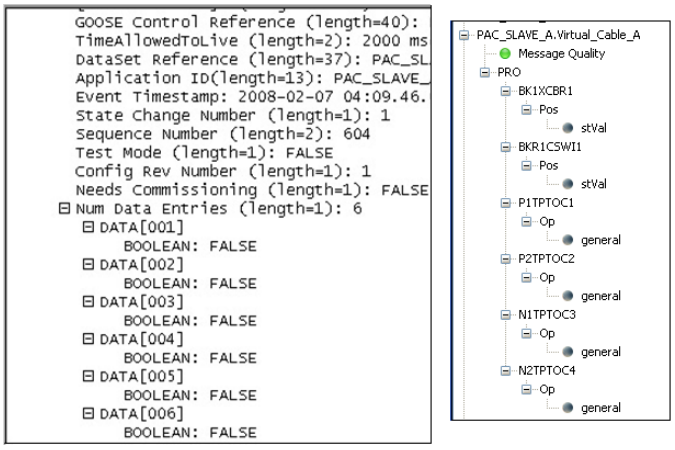

Fig. 5. GOOSE data verification

In order to keep the GOOSE multicast small and efficient, the GOOSE data set includes the present state of the data values but not their names. The Ethernet traffic capture decodes the individual data types (BOOLEAN, in this case) and their value (FALSE) but not the data names, which are available and shown in the configuration software.

Other information about this GOOSE message is compared with another view from the configuration interface, which provides the multicast message naming and Ethernet parameters for one of the virtual cables documented in Fig. 1. The message configuration verification window is shown in Fig. 6.

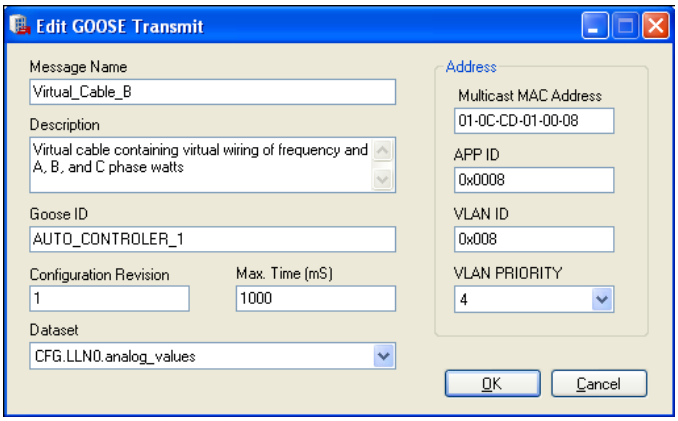

Fig. 6. GOOSE message configuration verification

C. GOOSE Diagnostic Report

Additional verification is done by communicating with the IEDs that are sending and receiving the GOOSE messages. Each end of the GOOSE cable is constantly supervised by each of the subscribing IEDs, which calculate the GOOSE message quality. Fig. 7 is a screen capture of an IED GOOSE report command response showing the configuration information and real-time statistics for both transmit and receive GOOSE messages along with the present communications status. According to this IED, the single GOOSE transmit publication and all but one GOOSE receive subscription are normal, as evidenced by the lack of error codes. However, subscription to multicast 01-0C-CD-01-00-04 is failed with the TTL EXPIRED error code.

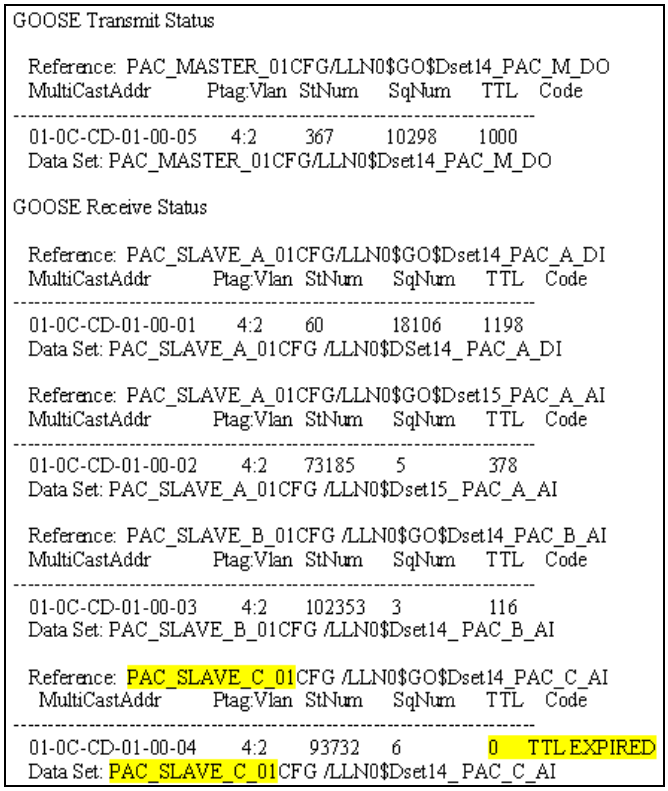

Fig. 7. GOOSE report command response

D. GOOSE Message Quality Calculation

GOOSE messages are published immediately after one of the values in the data set changes state or passes through a dead band. The repetition of the multicast becomes a maximum rate after the change, and if the payload then remains unchanged, the repetition rate slows until it reaches a preconfigured minimum repetition. The multicast will continue to publish at this slower rate until another data change occurs. Each time a GOOSE message is published, the IED calculates the time-to-live (TTL) value and includes it in the GOOSE message. TTL is a multiple of the maximum amount of time before the multicast message will be repeated by the same publisher. The publisher will not wait, but it will publish immediately if some data change.

Fig. 7 illustrates a GOOSE status report collected directly from an in-service IED in the quiescent state of no data change and GOOSE publication repetition at the least frequent. In this case, the least frequent rate is equal to the maximum time setting of 500 milliseconds, half the value of the setting of 1,000 milliseconds illustrated in Fig. 6 for a different virtual cable configuration. In the quiescent state, the IED publishes a TTL equal to twice the maximum time setting. In this case, the GOOSE with PAC_M_DO contents from Fig. 7 will be published twice as often as the GOOSE with Virtual_Cable_B contents from Fig. 6.

The value of 1,000 milliseconds for the PAC_MASTER publication TTL represents twice the maximum time setting and is the value published within the last outgoing GOOSE message. Subscribing IEDs use this TTL value as their time-to-wait (TTW). In the quiescent state, the IED publishes a TTL equal to twice the maximum time setting; during a data change sequence, it is triple. This is done to avoid nuisance alarms due to the nondeterministic nature of Ethernet. This TTW is the time that a subscribing IED will consider the data from the GOOSE virtual cable valid. This allows for some variation in delivery time but still indicates a problem after a delay of multiple publication intervals.

Fig. 7 also illustrates the present state of the TTL values for GOOSE messages being received by the PAC_Master. At the time that the report was generated, the PAC_Master was expecting a new GOOSE message for PAC_A_DI within 1,198 milliseconds, PAC_A_AI within 378 milliseconds, and PAC_B_AI within 116 milliseconds. The error code, TTL EXPIRED, for the PAC_C_AI GOOSE receive status at the bottom of Fig. 7 suggests that the PAC_MASTER waited a time equal to TTL and timed out while waiting to receive the next multicast message from IED PAC_SLAVE_C. This error code will remain and the data mapped to the internal IED logic will be unchanged until the next correctly configured multicast message is received. This error indicates that the IED sending this message has either stopped transmitting this message and/or the network connection between the IEDs is not functioning properly. Additional checks can be made at this point to further troubleshoot and isolate the issue. For example, if another IED is successfully subscribing to IED PAC_SLAVE_C, it is a network problem and not a problem with the publishing IED.

Additional error codes are shown in this display for this or other GOOSE messages when errors occur with the network or sending devices. Table I lists other possible error codes and their descriptions.

TABLE I
GOOSE MESSAGE ERROR CODES

Message Statistic	Error Code
Configuration revision mismatch between publisher and subscriber	CONF REV MISMA
Publisher indicates that it needs commissioning	NEED COMMISSIO
Publisher is in test mode	TEST MODE
Received message is decoding and reveals error	MSG CORRUPTED
Message received out of sequence	OUT OF SEQUENC
Message TTL expired	TTL EXPIRED

In addition to the GOOSE report command response to give indication of GOOSE message health, many IEDs calculate a logical indicator of this same status. This logical indicator is then used in IED logic to alarm and/or enable alternate logic during the period of message quality issues. Line 9 in Fig. 1 describes mapping the supervisory status of the message quality of Virtual_Cable_C to virtual bit VB009 in the TRANSFORMER_RELAY_1. Fig. 8 shows a GOOSE message configuration screen with the message quality element being assigned.

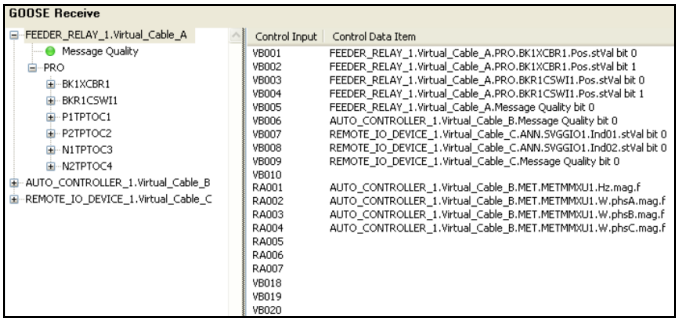

Fig. 8. GOOSE message quality

Fig. 9 illustrates the use of message quality to supervise the status of a GOOSE message virtual cable between a feeder relay and a transformer bay controller. The power transformer secondary protection cannot be coordinated with the feeders without fast and constant block indications from feeder overcurrent relays. GOOSE messages communicate the block information, enable coordination, and allow the definite-time overcurrent element in the power transformer secondary relay to be enabled with a much shorter delay. In addition to the block signal from the feeder, the loss of GOOSE virtual wiring, which is detected as bad message quality, appears in the logic selectivity scheme to block the trip of the fast overcurrent element of the power transformer secondary relay, as shown in Fig. 9. In the case of a communications system failure, the value of the message quality error code is set to 1 as a result of TTL expiration. This loss of the blocking signal creates an uncoordinated condition, and the power transformer secondary protection reverts to the longer traditional coordinating scheme operation time.

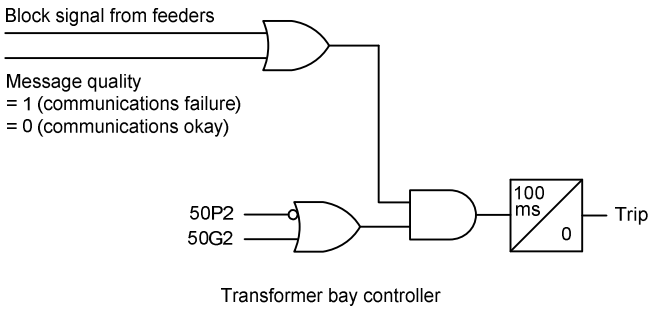

Fig. 9. Communications-aided bus protection logic

E. Virtual Wiring Multicast Message Construction and Network Navigation

Multicast behavior means that each time a multicast message, such as GOOSE, is received on a switch port, it is automatically sent to every other port. This becomes a huge burden on the switch to manage more traffic. Unneeded but unstoppable messages waste bandwidth on network segments where they are not required but are automatically sent and also increase latency of necessary GOOSE exchange. IED processor burden increases because the IED must process each of the necessary and unnecessary GOOSE messages that are received.

Each time an IED receives a multicast or broadcast message, it has to decode the message and determine if it should process the message. The IED examines the multicast address, data set reference, application ID, and GOOSE control reference of each message to verify that it is the correct message from the correct IED. If it matches the IED subscription configuration, the IED processes and maps the contents to internal memory. If it does not match, the message is discarded after the verification processing.

One of the techniques to alleviate the network burden of multicast messages is the VLAN. IEEE extended the Ethernet Standard 802.1 with the designator Q for message quality, which includes extensions for optional VLANs via a previously unused field in the Ethernet header tag. IEEE 802.1Q VLAN, or QVLAN, divides a physically connected network into several VLANs, as shown in Fig. 10. QVLANs originated from a need to segregate network traffic from different departments inside one enterprise. While keeping the sensitive information private, QVLAN techniques can restrict traffic flow of multicast messages to a single QVLAN and therefore the devices within it.

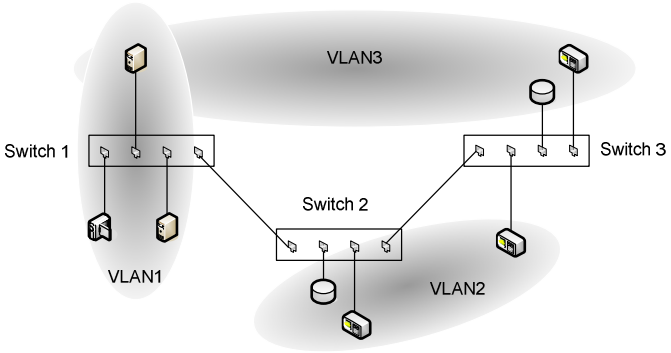

Fig. 10. Switched Ethernet and QVLAN configuration

IEC 61850 adopted the use of QVLAN tags to identify multicast messages and overcome the inability to perform network routing by performing manual routing. Because of the unwanted and unstoppable automatic distribution of multicast messages, the manual routing performs in reverse. The multicast messages are routed everywhere but are only allowed to pass through ports from which they have not been blocked. In IEC 61850 networks, QVLAN tags are implemented within the multicast message by the publishing IED, potentially used by switches for manual routing, and ignored by the subscribing IEDs.

Another feature of the QVLAN is that it becomes the unique cable designator. Ethernet switches use the QVLAN to cause the Ethernet network to act as power system engineers wish and guide the GOOSE virtual cable to only those IEDs that need it. Network designers add settings to each switch port to identify which QVLANs to allow and which to restrict. Fig. 6 illustrates the configuration of a GOOSE message used as Virtual_Cable_B with the unique VLAN ID set to 0x008. Best engineering practice procedures suggest setting the last octet of the multicast MAC address, APP ID, and VLAN ID to the same value (0x008 in this case).

Another compensation technique that was adopted to reduce transit latency of multicast messages because of network congestion is the use of priority tagging per IEEE 802.1p. In order to compensate for the bandwidth-sharing techniques of Ethernet, packet prioritization was created to emulate long-standing SRO serial protocol message prioritization methods. In this case, each packet, regardless of the protocol within it, is assigned a priority. This is done similar to QVLAN within a previously unused field in the Ethernet header tag. For switches and IEDs that support the feature, the priority tag indicates the importance of each packet relative to the others. Packets with the highest priority are sent to the top of the queue. If a lower-priority message is in process or packets with the same or higher priority are in queue, even prioritized packets must wait. Fig. 6 illustrates the

configuration of a GOOSE message used as Virtual_Cable_B with the VLAN PRIORITY set to 4 (out of 7).

An important note is that latency because of the incorrect use of the priority tag may not be evident during normal operation of the network. Latencies may occur only during times of power system and Ethernet network stress, long after commissioning testing, at the time when latencies are most dangerous. The only effective method to segregate Ethernet multicast traffic and GOOSE virtual cables is to follow these simple rules:

- Assign each GOOSE virtual cable a unique QVLAN.
- Allow no multicast messages on the network without QVLAN tags.
- Assign each GOOSE virtual cable an IEEE 802.1p priority tag.
- Disable all unused switch ports.
- Configure every switch port to block delivery of every multicast message to the connected IED except the QVLAN virtual wires that the IED has subscribed to within its configuration file.

F. Virtual Wiring Point Verification

Additional checks are needed to validate the individual data items being communicated via peer-to-peer digital communications interconnections. These checks require internal point monitoring in the receiving and transmitting IEDs. Using the configuration tools of the IEDs, additional checklists and logic mapping diagrams can be created, as shown in Fig. 11.

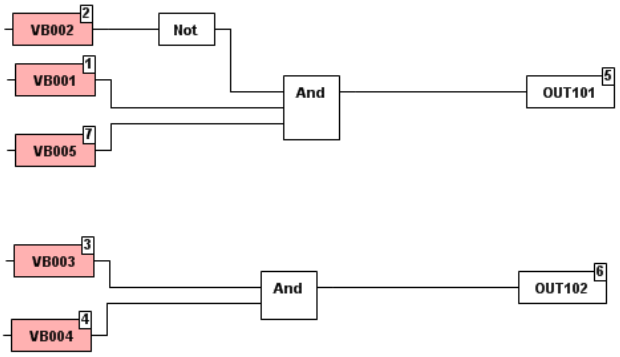

Fig. 11. GOOSE logic mapping example

From this information, applications can be created to display GOOSE diagnostics as well as the data set contents from each IED. Fig. 12 shows an example display of GOOSE diagnostic data built into a substation HMI [1]. These displays identify and verify the virtual connections among IEDs. In this example, the present values conveyed by virtual wiring in the virtual cable, LS BAY 1 LINE 1 B RECEIVE DATA SET 1, are compared to the expected values. This troubleshooting tool identifies and highlights a discrepancy for further evaluation. This essentially replaces a voltmeter checking the continuity of a physical wire termination.

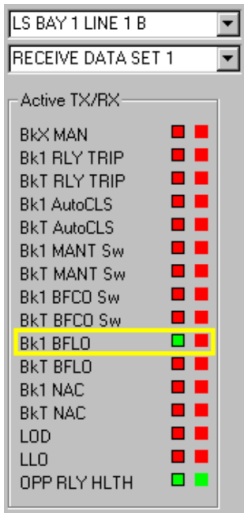

Fig. 12. GOOSE diagnostic data

V. Essential Device Monitoring Tools

The nature of GOOSE messaging requires specialized processing in the transmitting and receiving IEDs. GOOSE is not standard TCP/IP messaging but is only a Layer 2 implementation. It uses a unique Ethertype and is size-limited to a single Ethernet frame.

A. GOOSE Message Statistics

Each consecutive GOOSE message contains a unique sequence number that is incremented by one for each successive transmission. By monitoring this value, the subscribing IED determines if GOOSE messages are received out of sequence. Each GOOSE message also contains a state number, which is incremented each time an item in the data payload changes. When the state number is incremented, the sequence number resets to zero. The combination of state and sequence numbers allows the subscribing IED to determine which message it has received and determine if the message payload has changed.

B. GOOSE Message Failure Alarm and Notification

The IED receiving GOOSE messages calculates the message quality for each incoming GOOSE message. Because the GOOSE message format and methods are standardized, any IED receiving GOOSE messages is capable of calculating the GOOSE message quality for messages from any vendor IED.

Once the IED has calculated the GOOSE message quality status, this value is available as a logic element within the IED. The IED can use this status to block and enable logic, as discussed in the previous example. IEDs can also display GOOSE statuses on their front panels to aid in local troubleshooting and alarm via SCADA protocols, email, or other methods. Because this quality is an internal logic point in the IED, the change of status of the message quality is also time-stamped and recorded as a change of state event SER report in the IED.

C. GOOSE Message Reliability and Channel Availability

The aggregate of failure duration over a given amount of time determines the channel availability. IED-specific statistics are calculated within the IED as the GOOSE message quality status for each message representing the collection of possible error states and conditions. Once recorded as a time-stamped change of state, the GOOSE message quality status for each message is collected as a system-wide diagnostic. After commissioning, message quality will only fail when a message is corrupted or not received. The observation of failures will indicate the reliability of individual GOOSE virtual cables. If the message quality failure is intermittent, the duration of the failures is calculated as the difference between time stamps.

The IED can monitor and accumulate these individual error states as a count, indicating how many of each type has occurred since the last status reset. This provides IED-specific troubleshooting statistics. In addition to simple counts, some errors can also be timed, such as a TTL time-out error, to when the next valid message is received. These accumulated times can be used to calculate the channel availability. The observation of failures will indicate the reliability of individual GOOSE messages and/or the network connections between IEDs sharing GOOSE messages. Each IED can verify the performance of the incoming GOOSE subscriptions by monitoring the sequence and state numbers of the incoming multicast messages. Comparison of these statistics among multiple IEDs subscribing to the same multicast will reveal weaknesses in the Ethernet network segments that would otherwise be undetectable.

D. IED Time-Stamp Accuracy

Most early adopters of IEC 61850 used it to perform simple substation automation system (SAS) functions like SCADA. Those satisfied with ±5-millisecond time-stamp accuracy deploy Simple Network Time Protocol (SNTP) but rarely confirm its performance because it is difficult to test.

To address power industry needs for accurate timing and synchronization over Ethernet networks, the Relay Communications Subcommittee (H Subcommittee) of the IEEE Power System Relaying Committee (PSRC) and the Data Acquisition, Processing, and Control Systems Subcommittee (C0 Subcommittee) of the IEEE Substations Committee (Sub) established the joint Working Group PSRC H7/Sub C7, tasked to develop IEEE PC37.238 Standard Profile for Use of IEEE Standard 1588 Precision Time Protocol in Power System Applications. The joint working group coordinates its work with IEC Technical Committee 57 WG10 to enable adoption of the standard profile into IEC 61850 Edition 3.

IEEE 1588 is not yet standardized, and the accuracy of off-the-shelf SNTP is not adequate for any power system application. Network designers presently use IRIG-B, a Global Positioning System-based (GPS-based) method, also documented in IEC 61850. IRIG-B provides greater than 1-millisecond accuracy and is communicated to the IED via a connection to a time-distribution network that is physically separate from the IED connection to the Ethernet communications network.

IEC 61850 documents different levels of time-synchronization accuracy for different applications. Because there are numerous protocols and reasons for using communication, there are different classes of both message transfer speed and time-stamp accuracy. Further, the standard dictates that "the time synchronizing of the clocks in IEDs has to be one order of magnitude better than requested by the functional requirements" [4]. The classes of functional accuracy within the standard include: ±1 millisecond, ±0.1 millisecond, ±25 microseconds, ±4 microseconds, and ±1 microsecond. Therefore, even for the least severe accuracy class of ±1 millisecond, synchronizing of the clocks must be one order of magnitude better, which requires minimum accuracy of ±0.1 millisecond.

To date, the GPS-based method of a separate IRIG-B distribution network is the only method within the standard that is suitable to provide the accuracy necessary for messaging on a local-area network (LAN). Testing of commercial SNTP time-source clocks used in IEC 61850 SASs reveals that they are not sufficiently accurate, even for the least precise applications of ±1 millisecond.

In lab testing with commercial clocks directly connected to the IED, results demonstrate that the clocks drift from absolute time and also fail to provide ±1 millisecond or better synchronization of the IED clock via SNTP. However, this is not evident without specific observation. Though difficult to verify, it is a crucial mistake made by several SAS designers because the data within the SAS cannot be used synchronously. Further, archived event data will not accurately represent the true sequential events observed by several devices because their clocks will not be accurate to absolute time nor relative to one another. Essentially, waveform and SER time-stamp information will not be accurate enough to coordinate among networked devices.

These clocks that are routinely used within SASs have been verified to exhibit the following behavior:

- Time latency between IED time request and clock response exceeds 5 milliseconds one or more times within each 60-minute test period when communicating via a direct LAN cable between the clock and IED.
- This delay often exceeds 5 milliseconds and occasionally exceeds 30 milliseconds, which results in SNTP time errors exceeding 15 milliseconds.
- Methods like SNTP will change in accuracy as the network grows in size or utilization.

After verification of insufficient accuracy from commercial time clocks, a custom clock using different operating principles was built. Additional customization was performed in a specific IED. Proprietary improvements to the SNTP clock and IED SNTP interface yielded acceptable results of ±15-microsecond accuracy.

Without test points to verify accuracy and indicate that synchronization is lost, SAS data will not be accurately recorded, and this will remain unknown to users of the

information. Further, synchrophasor and process bus applications will be impossible without both LAN capability and confirmation of high-accuracy synchronization.

It is not obvious if the time-synchronization accuracy of a network is not satisfying the standard or how to verify accuracy. In fact, commercial clock vendors suggest that these same products are used to synchronize protective relays and other IEDs, as well as SCADA systems all around the world in thousands of installations. It is not clear if or how network designers test and verify accuracy in these networks.

VI. Conclusion

The act of integration realizes significant system benefits over traditional methods of measuring multiple field terminations, regardless of the protocol(s) or communications media used [5].

Systems constructed with integrated IEDs networked via Ethernet connections combined into a LAN offer the following key benefits:

- By using IEDs that, in addition to their primary functions, also perform ongoing diagnostics of their own performance and that of the equipment they are monitoring, the quantity of unsupervised process and apparatus functions is reduced.
- Supervision of digital communication allows data clients to differentiate between silence of field sensors and failure in the data collection path. This makes the data more dependable and more valuable to the various data clients. Supervision is maximized by replacing traditional, unmonitored copper terminations with monitored digital communications at the IED closest to the field data. This, in turn, detects and alarms communications problems immediately.

Direct-wired I/O can be easily replaced with an IED network and communications processors by using more functionality available in the IEDs and new peer-to-peer Ethernet methods from IEC 61850.

Commissioning tests with these new methods use new tools and documentation but follow the same process and visualization. Network test devices, HMI applications designed to observe network messaging, and internal IED diagnostics are all essential for configuring, verifying, and troubleshooting network communications.

Effective methods to segregate and verify GOOSE virtual cables include the following:

- Assign each GOOSE virtual cable a unique QVLAN.
- Allow no multicast messages on the network without QVLAN tags.
- Assign each GOOSE virtual cable an IEEE 802.1p priority tag.
- Disable all unused switch ports.
- Configure every switch port to block delivery of every multicast message to the connected IED except the QVLAN virtual wires that the IED has subscribed to within its configuration file.
- Use the ping command between IEDs to verify network path navigation.
- Use test mode elements within the GOOSE data set to provide isolation of each specific virtual wire for testing rather than the entire virtual cable.
- Confirm the LAN-based time synchronization with direct-connect IRIG-B time error detection.
- Use GOOSE state and sequence number statistics.
- Use GOOSE message quality to supervise virtual cables and create adaptive communications-aided IED logic.
- Create IED front-panel alarms, SCADA, alarms, email, and phone calls directly to those that need to know of failure of virtual cables.
- Create virtual wire point lists for use in commissioning.
- Use Ethernet network analyzers to confirm virtual cable performance and payload.
- Choose multivendor IEC 61850 configuration tools.
- Use onboard IED reports for real-time verification of device configuration and IEC 61850 SCL configuration.
- Use onboard IED GOOSE reports to confirm subscription and publication configurations, message statistics, and error codes.

VII. References

[1] H. Fischer, J. Gilbert, G. Morton, M. Boughman, and D. Dolezilek, “Case Study: Revised Engineering and Testing Practices Resulting From Migration to IEC 61850,” proceedings of the 18th Annual DistribuTECH Conference and Exhibition, Tampa, FL, January 2008.

[2] K. Zimmerman, “Commissioning of Protective Relay Systems,” proceedings of the 34th Annual Western Protective Relay Conference, Spokane, WA, October 2007.

[3] J. Young and D. Haas, “The Importance of Relay and Programmable Logic Documentation,” proceedings of the 2008 DistribuTECH Conference and Exhibition, Tampa, FL, January 2008.

[4] IEC 60870 Standard. Available: http://www.iec.ch.

[5] E. Udren and D. Dolezilek, “IEC 61850: Role of Conformance Testing in Successful Integration,” proceedings of the 8th Annual Western Power Delivery Automation Conference, Spokane, WA, March 2006.

VIII. BIOGRAPHIES

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

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, communications, 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 IEC technical committees tasked with global standardization and security of communications networks and systems in substations.

© 2010 by Schweitzer Engineering Laboratories, Inc.
All rights reserved.
20100729 • TP6437-01