Case Study Comparison of Serial and Ethernet Digital Communications Technologies for Transfer of Relay Quantities

Mike Gugerty, *Southern California Edison*
Robin Jenkins and David J. Dolezilek, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—This paper is a case study comparing the performance of multiple communications technologies and architectures available via protection and automation intelligent electronic devices (IEDs) for use in monitoring and controlling Remedial Action Schemes (RAS). The discussion includes the design description and implementation issues of several popular and standardized technologies available today to perform high-speed digital communications of data among IEDs.**

Discussion of the characteristics of each type of communication is combined with test results from an actual installation in a customer facility. Tests were performed in a lab environment and also over a wide area communications system. The goal was to understand the benefits of using protective relays and automation IEDs to improve the customer's RAS monitoring and mitigation capabilities, while at the same time, enhancing diagnostics and reliability and reducing costs. The customer is using the test results to evaluate the best method to provide relay-to-relay communications for internal and intertie RAS systems. The results are applicable to any use of high-speed digital communications to transfer data among IEDs. The various technologies are compared based on the customer selection criteria of reliability, simplicity, speed, expandability, and cost.

I. Southern California Edison's Reasons for a New RAS Approach

At Southern California Edison (SCE), RAS systems are implemented to ensure reliable power system performance following outages on a transmission grid network. They include fast, automatic control actions to mitigate thermal overloads and system instability upon the loss of one or more transmission lines. With these automatic protection features, RAS systems are used in place of expensive alternative measures, which include reconductoring transmission lines, building new lines, and/or adding new transformers.

SCE deploys local RAS systems throughout their transmission operating area, including 1,183 miles of 500 kV lines, 1,181 miles of 230 kV lines, and 350 miles of 115 kV lines. Supporting these main transmission corridors are several independent localized RAS systems with more systems under development and the potential to add a multitude of new systems based on recent generator queue studies.

Looking at these numbers gave SCE a reason to reevaluate the design of their current system implementation. In the past, each local RAS system deployment required rework of the following:

- Planning
- Design
- Programming
- Implementation
- Support

Because each RAS system design is influenced by the components that monitor and protect the power system at a specific location, replicating previous control designs was very simple. However, the fact that the equipment providing communications connections to the wide area network (WAN) is often unique at every location makes replication of communications parameters in the multiplexer equipment difficult. Arming, disarming, and testing these systems require manual coordination between the regional control center, energy management system, communications systems, Protection department, and substation staff. Covering the maintenance of many unique communications installations over this large geographical area is very time consuming.

Perhaps most important was the anticipation of creating RAS systems that cover very large areas. These newer systems will need to not only accept many messages simultaneously from many remote locations but also process each message and then the associated RAS logic. The logic processor presently being used by SCE, with success in small RAS designs, does not have enough logic capabilities to handle the large wide area RAS systems envisioned for the future.

All of these factors encouraged SCE to perform the research necessary to develop a new "centralized" RAS system design. Communications of new or existing protocols over Ethernet presents the opportunity to use a traditional computer as the central processor. Separately research will identify what kind of computer (standard, server, ruggedized etc.) and software applications to use. Demonstrating that the protocols can travel over Ethernet simplifies the logic design so that SCE can use off-the-shelf software applications and standard hardware interfaces to receive and process numerous RAS messages from remote locations. Using Ethernet simplifies the computer hardware because one Ethernet interface can serve the same function as numerous individual serial ports for direct serial connections. The new design is also intended to help avoid the customization required to implement individual local RAS communications systems, allow centralized coordination of arming, disarming, and system testing, and simplify coordinating system maintenance. Reliability is expected to improve with capabilities to monitor end-to-end grid parameters and quickly respond to abnormal conditions. The area of

mitigation will expand from a few local choices to all nodes included within SCE's system, including dynamic load shedding/generation tripping and improved management of load restoration.

Separate from the protocol research, SCE is evaluating a centralized processor capable of supporting the required number of Ethernet or serial connections, while also performing centralized processing for the wide area RAS.

II. Present Technology

A. RAS Communications Protocol

The traditionally installed localized RAS systems utilize IEDs to detect abnormal system conditions, communicate them to remote IEDs, and together, determine the appropriate action to prevent unwanted outages. Communications speed and reliability are critical factors to ensure proper system operation. SCE's RAS IEDs exchange data using a peer-to-peer Robust Serial RAS Protocol, communicated over an assortment of communications systems. The term Robust Serial RAS Protocol (RSRP) refers to the MIRRORED BITS® communications protocol, which is a serial communications technology that exchanges the status of Boolean and analog data, encoded in a digital message, from one device to another. This inexpensive, highly secure technology is used in numerous protection, control, automation, and monitoring applications within SCE as well as around the world. This protocol was chosen because of its inherent reliability and security features essential to operating a dependable RAS system. Many of the in-service RAS system IEDs came equipped with one or more dedicated communications interfaces supporting the RSRP. In addition to performing protective relaying functions, these IEDs have extended digital inputs and outputs, multiple RAS protocol communications interfaces, annunciator LEDs, and a communications alarm contact to indicate intermittent or total RAS communications failures. RAS IEDs that do not natively speak this RAS protocol are hardwired directly to other relays that do support the RSRP for easy integration into the system. Another possibility would be to hardwire outputs of these RAS IEDs, which do not natively support the RSRP, to a simple interface module that translates the RSRP into digital input and output contacts.

The RAS protocol accomplishes 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 input or is mapped directly to a control output.

This protocol is also capable of sending up to seven analog values between IEDs. This obviously presents the opportunity for different, more sophisticated RAS schemes than were necessary for this SCE application.

All transmit bits (TMBs) are processed during each IED processing interval. The status of each TMB is reflected in each transmitted message. When the message is received by the remote IED, each received bit (RMB) is treated as a logic input, which is programmed for RAS protection, automation, control, or monitoring functions. Messages are transmitted and received asynchronously at rates of up to 9600 baud. SCE uses this protocol over several communications media including dedicated optical fiber, multiplex digital networks, and analog microwave.

The receiving IED checks each received RSRP message 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 it 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 they are not inadvertently miscabled in the field.
- Messages received prior to timeout

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.

B. Integrating RAS IEDs Not Compatible With RSRP

Not all SCE RAS IEDs include support for the RSRP. To integrate these relays, as mentioned previously, SCE hardwired their outputs to the input contacts of other relays that support the RSRP. SCE also integrated inexpensive RSRP I/O modules for use as annunciators via LEDs that visualize bits received from the RSRP.

C. Similarity Between RSRP and Other Wide Area Protocols

The implementation of the RAS protocol as a point-to-point protocol closely matches the implementation of several synchrophasor protocols. Synchrophasors are becoming a very important consideration for future wide area protection and control strategies. The fact that the RAS protocol and synchrophasor protocols are implemented as point-to-point connections will simplify installations that include both protocols. This functional similarity makes the implementation, design, and troubleshooting of the combined protocols more compatible.

D. Present Installation Challenges

SCE has many different kinds of communications multiplexer equipment from multiple vendors installed throughout their system. Each different multiplexer requires a unique serial communications interface and a different group of settings for installation. SCE was searching for a way to simplify each installation and make them more similar. They wanted a more uniform solution that could be used at many locations throughout their service territory. Due to the variety of presently installed multiplexer equipment, it was not possible to install the same EIA-232 MUX Module at each site. Had this

been possible, it may have accomplished the desire to standardize installation practices.

Although SCE is satisfied with the performance, cost, and reliability of the present RSRP over serial connections, they were interested in investigating ways to pass this protocol, or other wide area RAS protocols, over Ethernet instead of serial connections.

The existing SONET provisioning establishes links between endpoints via a telephone-type exchange, which allocates dedicated 64000-baud channels. Individual channel provisioning establishes the available bandwidth in advance, thus providing predictable performance. However, once allocated, unneeded bandwidth is left unused.

Ethernet is actually established over SONET by provisioning one large channel to be shared by all Ethernet traffic. This results in less predictable channel performance; however, bandwidth unneeded by one conversation is available for use by other conversations. So all Ethernet conversations share the available bandwidth, and traffic is routed to the correct endpoint without dedicated channels for each conversation.

The simpler, although less predictable, Ethernet channel provisioning over SONET was expected to make replication of communications designs possible. This, in turn, would make installations at different locations similar and simpler.

III. Changing the Installation Approach

A. Simple Acceptance Criteria

As SCE prepared to investigate other communications technologies, they documented a simple test and acceptable performance of the test.

The acceptance criteria included that the IEDs must perform a three-IED RAS scenario in 50 ms or less over WAN Ethernet connections, while at the same time satisfying cost and reliability parameters. The designated WAN connections were simulated as messages traveling roundtrip between Los Angeles and Bakersfield, California—a distance of roughly 230 miles. Therefore, each message must travel 460 miles between IEDs with an Ethernet connection at each end. The test duration was measured by an oscilloscope in the black box fashion to be the time between energization of the contact input that triggered the beginning of the test and energization of the contact output indicating its completion.

For this test, average times of several consecutive tests were used for comparison.

B. Simpler Installation Using Direct IED Ethernet Connections?

It was SCE's hope that migrating to Ethernet would simplify installations and make them more similar. To that end, SCE felt that by adding Ethernet connectivity to their existing IED schemes, they would benefit from reuse of all their existing logic and reduce design and commissioning of RAS communications.

C. Maximize Use of High-Speed Network

SCE was fortunate that Ethernet installations at or near their substations were becoming prevalent. These installations were capable of much higher communications interface speeds than the previously used serial channels, even though the WAN SONET equipment remained the same. SCE wanted to investigate if a higher bandwidth communications interface would improve RAS performance without sacrificing reliability or dependability.

D. Considering Multiple Vendors

SCE has a large service territory with many interconnections to other utilities as well as many large customer tie points. During this investigation, they decided to explore other protocols that were native within a wider range of IEDs. The thought was that this might simplify RAS interconnections if there were more IEDs from which to choose. SCE was encouraged by the fact that the initial components of the IEC 61850 standard had recently been ratified and that others were thought to soon be complete. Although satisfied with the performance of the existing RAS protocol, SCE decided to also test direct Ethernet connections and a protocol common among multiple vendors, which appeared to be IEC 61850.

IV. Selecting RAS Messaging Over Ethernet

A. Tunnel Existing RAS Protocol

SCE tested relays used in their existing RAS schemes by adding serial-to-Ethernet transceivers to IEDs communicating the RSRP serially and "tunneling" RAS messages over the WAN communications system. Tunneling is a term for moving serial protocols over Ethernet between definite endpoints rather than simply broadcasting them to multiple endpoints as with some Ethernet protocols. This is done by configuring the transceivers as a pair that pass messages to each other. The RSRP is well suited to tunneling because it is a protocol with dedicated endpoints rather than being sent as a broadcast. When each of the multiple IED ports are configured to communicate the RSRP, unlike several other available protocols, it is configured to act as half of a pair and will only interact with its partner. This prevents accidental, incorrect cabling, which may cause unwanted operations based on valid messages being received by the wrong IED or wrong connection to the correct IED. The RSRP is also used in a rebroadcast method, similar to broadcast of other Ethernet protocols, by use of a RSRP switch, which collects and transfers data among several IEDs.

The advantages of implementing the RSRP architecture include simple configuration, use of existing installed IEDs, and the continued use of the reliability and diagnostic features of the existing RAS protocol.

B. Hypothetical Use of Multiple Vendors

SCE recognized that choosing IED vendors was a lot more involved than choosing from those that support IEC 61850. Vendors are chosen based on customer service, product quality, delivery availability (time between order and receipt), vendor innovation, product price, and product features. In this case, the product features compared were in support of the RSRP and IEC 61850 protocols. SCE did not plan to change IED vendors; however, they did want to confirm that the in-

ternational standard IEC 61850 protocol was widely available. They recognized that they may not be choosing the IEDs to be used at each intertie point in each RAS scheme.

C. IEC 61850 GSE

Peer-to-peer messaging within the IEC 61850 standard is accomplished with two similar compliant protocols that differ slightly. These two protocols, IEC 61850 GOOSE (GOOSE) and GSSE, are collectively referred to as GSE. GSSE (also known as UCA GOOSE protocol) has been available from a couple vendors for many years, including the vendor providing the existing RAS protocol [1].

Note: 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 will not communicate with a GOOSE session on another IED. SCE chose to consider use of GOOSE only.

One driving force behind the creation of IEC 61850 was to better accommodate interoperability among IEDs from multiple vendors. The standardization of GSE messages ensures interoperability directly between IEDs for protection, interlocking, and automation. Although the two messages are different, they can both exist on the network and provide interoperability between multiple devices that support GSSE and/or between multiple devices that support GOOSE, or both. Further, the content of both protocols was sufficient to satisfy the RAS system requirements.

SCE learned that many vendors had not implemented UCA or GSSE protocols and, therefore, were very new to the market. Products from these vendors do not have the years of proven experience with Ethernet operating in the substation environment. The vendors that offered early support of UCA have years of experience providing substation Ethernet and can provide observed reliability information. Therefore, the track record of field-proven IED Ethernet performance was added to the list of vendor comparisons.

In order to maximize the pool of available IEDs, SCE chose to evaluate only the GOOSE protocol.

D. Is IEC 61850 Truly Available From Multiple Vendors?

1) Questionnaire

In order to learn directly from vendors what products were recommended for use within their RAS scheme using GOOSE, SCE sent a questionnaire to individuals for several vendors identified as contacts through commercial discussions and the UCA International User's Group web page (UCA International administers the marketing for the IEC 61850 standard). SCE successfully sent questionnaires to the following vendors identified as potential suppliers. Other supplier contact information was inaccurate or unavailable.

- ABB
- AREVA
- Cooper
- GE
- RFL
- SEL
- Siemens
- Team Arteche
- Toshiba
- ZIV

SCE also asked about product pricing and configuration methods.

2) Questionnaire Summary

All but one of the vendors listed above replied to SCE. Out of those nine responses, nine vendors documented having GOOSE protocol available in products as of July 2006, with one vendor documenting that they support it through their own vendor proprietary method. However, none of these nine vendors supported extracting analog values from the GOOSE message for use in the IED. Therefore, a GOOSE RAS, from among those surveyed at the time of this publication, is not capable of exchanging analog data among IEDs. This is a major difference between GOOSE and the RSRP, which exchanges up to seven analog values.

A synopsis of the questionnaire is included in the Appendix, and a summary of the responses given is included below.

- The average price to add one copper Ethernet interface was $701 based on six responses.
- The average price to add IEC 61850 was $873 based on four responses.
- Only one vendor documents having IEDs that support the RSRP directly.
- Only two vendors document having Ethernet and GSE available and in use for several years.
- Only four vendors document having support for standard engineering access through the Ethernet port, the others require proprietary protocol and/or serial connections.
- Only four vendors document having support for non-IEC 61850 SCADA protocols through the Ethernet port, the others require proprietary protocol and/or serial connections.
- Only three vendors document having the ability to publish eight or more GOOSE messages, the others may not be capable of true RAS schemes.
- Seven vendors document having support for non-Boolean data in their GOOSE data sets, such as analog values, which will be useful in sophisticated RAS schemes.
- All vendors document having support for priority tagging for optimizing latency through Ethernet switches.
- All vendors document having support for virtual LAN (VLAN) identifiers to facilitate segregation of GOOSE traffic on the Ethernet network.
- Six vendors document allowing editing of the data sets published in the GOOSE messages so the user can send what they choose.
- Only three vendors document having support for configuring the IEDs by loading a CID SCL file as specified in the IEC 61850 standard.

- Five vendors document having configuration software that can import and understand SCL files from other vendors to facilitate configuring GOOSE messages between vendors.
- Only one vendor documents having the ability to confirm which configuration file is active in the IED.
- Only two vendors document having the ability to confirm which GOOSE messages are being successfully sent and received while in service.
- Only four vendors document having support for six or more client associations, the others may not be capable of supporting all the protocol gateway, HMI, and engineering access connections required.
- Only two vendors document having the ability to remotely load IEC 61850 configuration, which is essential when the configuration engineer is remote from the substation.
- The RSRP I/O module will interface with IEDs from each vendor (this is demonstrated by the operation of the module and not as a result of a question to the vendors).

V. Message Performance Analysis

A. Speed and Control Timing

The effective operation of a centralized RAS system largely depends on the time required to remotely detect an abnormal condition and respond with a decision-making control action(s). Because of the geographical area that SCE's RAS system covers, response time becomes critical to the success of the system. As mentioned previously, using their experience designing local RAS systems, SCE established a benchmark of 50 ms to detect and respond with a RAS control(s) action in the three IED scenarios. This time includes remote detection of an abnormal condition, transmitting an alarm 460 miles over a WAN to the centralized RAS controller, determining the proper action, and then transmitting this action(s) 460 miles over a WAN to the appropriate remote RAS IED(s) where the control action(s) is implemented.

B. Test Description

The test involves three IEDs communicating to each other peer-to-peer. IED1, the Monitor IED, is monitoring line conditions and, when appropriate, after a line-open condition is detected, sends a Status message to IED2, the Central Logic Processor IED. The status of the RAS armed or disarmed permissive is resident in IED2 as is the logic to determine when to send a mitigation signal. The line-open condition is simulated by energizing an input contact on IED1. Upon receipt of the Status message from IED1, IED2 extracts its content and, **if** the RAS is **armed,** performs a calculation to determine if remedial action is necessary. If IED2 decides to take action, IED2 sends a Mitigation command message to IED3, the Mitigation IED. When IED3 receives the Mitigation command message from IED2, IED3 energizes a trip output contact. This output contact is hardwired to an input on IED1. In this way, the total time duration is measured between detection of line one open as a contact input on IED1 and the eventual trip output of IED3 detected as a second contact input on IED1. The time duration was measured with a separate instrument and verified with internal sequential events records (SER).

SCE staged the test with IEDs from two different vendors, Vendor A and Vendor B, and tested three different protocols. These tests were completed on a LAN (all IEDs directly connected peer-to-peer or via local Ethernet switch) and across a WAN connection via a local Ethernet switch and Ethernet router.

GOOSE protocol messages were sent using a multicast group address and were, therefore, not routable over a WAN. In order to simulate WAN timing for the tests, SCE actually created a long LAN connection over the physical WAN connection, via the SONET system, between Los Angeles and Bakersfield, California. SCE recognized that, unlike the RSRP, the GOOSE protocol installations required logical LAN connections between all RAS locations. This raised severe security concerns that needed to be addressed separately.

IEDs from Vendor A were tested using the existing serial RAS protocol over a serial LAN, an Ethernet LAN, and an Ethernet connection to the WAN. Next, these same IEDs from Vendor A were tested using the IEC 61850 protocol over the Ethernet LAN and then the Ethernet connection to the WAN.

IEDs from Vendor B were tested using the IEC 61850 protocol over the Ethernet LAN and then the Ethernet connection to the WAN.

In addition to the RAS scenario test, peer-to-peer test results were calculated as the difference between the times that SER were timestamped in each IED. The IEDs were synchronized via IRIG-B, and SER were created in IED1 when it transmitted the alarm message and in IED2 when its logic received the result of the incoming alarm message from IED1.

C. Test Results

Table I shows the timing results of the tests performed. LAN and WAN peer-to-peer times were calculated based on SER records in the IEDs. All roundtrip time results for the "Three IED Test Scenario" were measured externally using a scope except for one. Because no EIA-232 MUX Module was available, values for Vendor A RSRP via Serial to WAN were calculated. The EIA-232 MUX Module vendor calculated a conservative worst-case 4 ms peer-to-peer delay and an 8 ms three-IED test delay using latency for the speed of light of around 5 μs per mile. These calculated results are consistent with actual observed performance.

TABLE I
IED TIMING RESULTS FOR RAS SCHEME PROTOCOL TESTS USING THE THREE-IED RAS SCENARIO

Vendor	IED PEER-TO-PEER	THREE-IED TEST SCENARIO
Vendor A GOOSE Protocol via Ethernet LAN	4 ms	13.3 ms
Vendor A GOOSE Protocol via Ethernet-to-WAN	9 ms	22.9 ms
Vendor B GOOSE Protocol via Ethernet LAN	14.3 ms	37.4 ms
Vendor B GOOSE Protocol via Ethernet-to-WAN	18.3 ms	45.4 ms
Vendor A RSRP via Ethernet LAN	14.6 ms	42.1 ms
Vendor A RSRP via Ethernet-to-WAN	22.6 ms	50.1 ms
Vendor A RSRP via Serial LAN	5.2 ms	14.7 ms
Vendor A RSRP via Serial-to-WAN	9.2 ms	22.7 ms

VI. MESSAGE RELIABILITY

A. GOOSE Broadcast/Rebroadcast

Unlike the existing RAS protocol, which constantly exchanges messages between IEDs, GOOSE protocol messages are generated for one of five reasons that include:

1. One or more of the Boolean contents of the GOOSE message data set experience a state change (system event).
   - In the case of the SCE RAS scenario test, the first GOOSE message was sent by IED1 as a result of the logic in IED1 recognizing energization of the input contact.
   - The second message was sent by IED2 as a result of the logic in IED2 processing the message from IED1.
2. One or more of the analog contents of the GOOSE message data set changes value by more than the reporting dead band.
3. The quality attribute of data associated with the contents of the GOOSE message data set changes value.
4. For reasons described later in the paper, the GOOSE protocol requires repetitive retransmission of messages described above (1 and 2). After the initial message, IEDs retransmit the same message repeatedly, usually for up to one second, in order to compensate for undelivered messages.
5. In the absence of a state change, GOOSE protocol messages are generated at preset time intervals to act as a heartbeat and confirm that the IEDs are still operational. This time interval is most commonly set to one second.

The GOOSE protocol has no standardized message acknowledgment mechanism. Due to the potential importance of each GOOSE message and the possibility of delay or incomplete transmission inherent in Ethernet networks, the IEC 61850 standard requires that each IED send multiple repetitive GOOSE messages in fast succession to increase the likelihood of message delivery. An exponential back-off mechanism is used, which gradually increases the time between messages until it reaches the length of the heartbeat-time interval.

Without a message receipt acknowledgement mechanism, the GOOSE protocol cannot be monitored for availability or dependability. Each successive GOOSE message is given a sequence number and a time-to-live value to aid receiving IEDs in message processing. The time-to-live value is compared to the time duration delta since the message was created. If the duration delta is larger than the time-to-live value, the message is considered "old" by the sending IED. The receiving IED can choose to use this indication as a validity check before it acts on data in the received message.

Although the GOOSE protocol does not provide message receipt acknowledgment, this feature can be built by the end user via custom logic in the IED. By configuring the IEDs to repeatedly and cyclically send GOOSE messages and monitor the receipt of each message, the IED logic can calculate channel performance [2].

B. RSRP Multimessage Redundancy Check

Reliable automation is dependent on reliable communications. This especially applies to a system responsible for making critical decisions directly affecting the stability of a regional power source. It is as important to know the validity of the data used to make the RAS decision, as it is to know the data value itself. In order to ensure reliability, the protocol used to transport the data should include self-monitoring features.

The existing RAS protocol messages are checked several ways to ensure data reliability. First, each byte of a received message is checked for parity, framing, and overrun errors. Second, all received messages, which are each repeated three times in the four-character message, are checked for redundancy. Third, the encoded message ID must match the receiving IEDs ID setting. And finally, at least one message must be received in the time it takes for three messages to have been sent or a network delay is detected. When received messages pass all of the reliability checks for at least two consecutive good messages, the receiving device asserts a valid communications status point used in the receiving IED's protection and control logic. This status is also to be monitored by the SCADA and other supervisory systems.

VII. COMMUNICATIONS DEPENDABILITY AND RELIABILITY

A. RSRP Message Security and Diagnostics Features

Once the RAS protocol passes all the reliability checks, it can be passed through user-configurable pickup/dropout security counters, where individual RMBs may be delayed for added security based on IED port settings. These security counters can be set from 1, which allows each bit to pass, to 8, which requires that a status change be consistent through 8 messages before the RMB status is allowed to change. This setting ensures that communications can be tuned to avoid nuisance alarms due to the characteristics of the communica-

tions network. If any of the protocol security checks fail, the start and end times of the disruption are recorded, and the difference is calculated as the disruption duration. If the disruption lasts longer than the customizable time duration threshold, the receiving IED asserts a communications disruption alarm. The duration is set based on the existing communications system performance to avoid nuisance alarms. The RAS communications channel unavailability is the ratio of the amount of time the channel is unavailable to pass messages (determined as the sum of all disruption durations) to the total recording interval time. This is calculated by dividing the aggregate of all outage durations by the total time span for a recording period and is presented as ppm unavailability.

The results from these security and diagnostic checks are used by the remote RAS IEDs and centralized RAS controller when determining critical RAS actions. They are also available to SCADA for use as communications and system maintenance alarms.

The RAS protocol is inherently point-to-point by design, physically and logically. When data from a single IED need to be sent to multiple IEDs, the RAS protocol is implemented as point-to-multipoint via a RAS protocol switch. This RAS switch broadcasts the data from one or more incoming RAS messages to multiple outgoing RAS connections. This configuration is implemented as several concurrent point-to-point connections both physically and logically. In both the single and multiple RAS data distributions, the logical and physical path of the messages are the same. This single message path leads to simpler design, installation, and troubleshooting, which, in turn, contribute to a more reliable and more easily maintained system. GOOSE, on the other hand, is actually a point-to-multipoint broadcast by design. It is possible to distribute this over a single crossover cable or one of many switch network topologies. The nature of Ethernet switching supports freedom of network configuration (i.e., star or mesh topology), regardless of the messaging destined for the network. This separation between messaging design and actual Ethernet network design means that the logical and physical path for GOOSE messages are not the same. This leads to a more complicated design and more complicated troubleshooting of the messages and their actual and intended destinations.

B. GOOSE Protocol

1) Lack of Message Security

The Ethernet-based IEC 61850 protocol does not currently include methods to automatically detect GOOSE message errors or include GOOSE communications performance and availability calculations. This is because messages are transmitted by exception, or at an infrequent rate, to support “heartbeat” or “watchdog” alarm detection.

2) Message Security Compensation

Logic can be added to detect if a heartbeat message is not received but not if a change-of-state message is not received due to the fact that they are sent on exception. Reference [2] illustrates the logic to perform a detection of failure to receive a heartbeat as well as a handshake mechanism for interrogating the state of an otherwise unresponsive peer. However, the main drawback of this approach was that there was no way to distinguish between a communications message loss and the absence of a system event (such as a line-open indication). Simple protection functions, such as traditional definite-time overcurrent, are prone to misoperation when implemented with the GOOSE protocol instead of the RSRP. This is due to the fact that simple communications message loss can lead to the clearing of the entire substation bus [2].

VIII. Message Processing Complexity

The RSRP was designed specifically for point-to-point data exchange between power system IEDs. The designers combined their skills in the art of protecting and automating power systems with their knowledge of the parameters of IED development to create a very concise and streamlined process. This process is detailed as follows:

A. Transmit RSRP Message

1. Detect change in relay logic intended for TMB.
2. Update new message with data.
3. Encode message.
4. Transmit message.

The quantity of lines of code (LOC) required to perform a function represent the complexity of the development, testing, and maintenance of the process. The total LOC required to transmit a RSRP message, Steps 2–4, is 100.

B. Receive RSRP Message

1. Receive message.
2. Validate message.
3. Decode message.
4. Transfer contents to host logic.
5. Detect change in relay logic intended for TMB.

The total LOC required to receive a RSRP message, Steps 1–4, is 360.

GOOSE messages were designed to serve many purposes on an Ethernet network based on the constraints of Ethernet interface hardware and network equipment. This process is detailed as follows:

C. Transmit GOOSE Message

1. Detect change in relay logic intended for GOOSE.
2. Detect change in GOOSE interface.
3. Store new value for each changed item.
4. Queue payload for use in GOOSE.
5. Determine changed data and update GOOSE.
6. Determine changed qualities and update GOOSE.
7. Update GOOSE message with date and timestamp.
8. Decompose message data to primitive types.
9. Encode contents using abstract syntax notation (ASN.1).
10. Encode GOOSE message.
11. Send GOOSE message.
12. Manage Ethernet transmit buffers.

The total LOC required to transmit a GOOSE message, Steps 2–12, is 4430.

D. Receive GOOSE Message

1. Manage Ethernet receive buffers.
2. Receive Ethernet frame.
3. Identify that content of Ethernet frame is a GOOSE message.
4. Push GOOSE message to queue.
5. Retrieve GOOSE message descriptor.
6. Decode GOOSE message.
7. Validate GOOSE message global quality.
8. Extract data from GOOSE message.
9. Validate GOOSE content quality.
10. Release decoded GOOSE data and Ethernet frame.
11. Update the GOOSE time-to-live timers.
12. Transfer GOOSE contents to host.
13. Transfer bit to host logic.
14. Detect change in relay logic intended for GOOSE.

The total LOC required to transmit a GOOSE message, Steps 1–13, is 3590.

Another measure of complexity is the size, in bytes, of the total message string necessary to move data between IEDs. It should be apparent that the message security, described previously, is useful only 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 message will 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 RSRP message, due to its concise design and transfer, is four bytes in length. GOOSE messages vary in size based on their flexible payload. However, a GOOSE message requires roughly 200 bytes to transfer a single RAS bit, which is 50 times larger than an RSRP message. It is, therefore, more susceptible to message corruption as a result of communications channel errors.

IX. System Reliability

A. IED Reliability

System reliability is greatly improved over traditional hardwired and tone gear RAS systems because the use of IEDs reduces the quantity of unsupervised process and apparatus functions. This is true with the use of IEDs that, in addition to their primary functions, also perform ongoing diagnostics of their own performance and the equipment they are monitoring [3]. However, the lack of message acknowledgement and deterministic message transfer within the GOOSE protocol creates shortcomings that should be overcome. The challenge today is that when this is left to logic in the IEDs, each solution from each vendor will be unique, configured separate from the communications configuration, and may not interoperate among vendors.

In addition to protocol link availability calculations, each RAS IED should include continuously run self-tests to detect out-of-tolerance conditions. These tests should run simultaneously with the protection, monitoring, and control logic, without degrading system performance. The RAS IED should report out-of-tolerance conditions as a status warning or status failure. For conditions that do not compromise the RAS IED, yet are beyond expected limits, a warning alarm should be generated and used by both the RAS IED logic and the centralized RAS controller. A severe out-of-tolerance condition should generate a status failure and enter an IED protection-disabled state. During this disabled state, protection elements and trip-logic processing should be suspended, all control outputs disabled, and a RAS IED disable alarm asserted. Both the status warning and disable alarm should be used by the centralized RAS controller when determining appropriate RAS actions.

B. IED Settings Complexity

The RSRP was designed to automatically exchange bits of information between IEDs as soon as the protocol is enabled. Therefore, after four simple settings in two IEDs, the IEDs will automatically exchange two sets of eight bits over two RSRP channels. Reliability and channel monitoring alarms and statistics will be calculated automatically.

GOOSE is not designed to begin automatically. It requires a minimum of thirty-three settings in the two IEDs to begin sending a single bit from one IED to the other. Sixty-six settings are required to exchange bits (i.e., one bit from IED1 to IED2 and a different bit from IED2 back to IED1). Then additional logic settings must be created to simulate the automatic reliability and channel monitoring alarms and statistics of the RSRP.

Though configuration software may automatically set some of the sixty-six settings, they are each required in order to exchange bits. This represents a much more complex configuration with more opportunity for error and, therefore, more complex troubleshooting.

C. System Reliability Analysis

Using fault tree analysis, the reliability of each type of system was calculated to compare relative dependability and uptime. The calculated expected downtime is a measure that identifies unreliability, lack of service of the RAS system, and the associated required maintenance effort to return the system back to service. Average observed reliability values were provided by Vendor A and the multiplexer vendor in the form of Mean Time Between Failure (MTBF) based on actual operational hours divided by failures for the population of in-service devices. Other reliability values represent average typical values provided by other vendors [4].

Device	MTBF
Vendor A Relay (observed)	300 yrs
Other Vendor Relay (typical)	100 yrs
Vendor A Ethernet Interface (observed)	2,500 yrs
Other Vendor Ethernet Interface (typical)	30 yrs
Vendor A Serial-to-Ethernet Converter (observed)	760 yrs
Other Vendor EIA-232 MUX Module (typical)	78 yrs
Other Vendor Ethernet Switch (typical)	30 yrs
Other Vendor Ethernet Router (typical)	28 yrs

The reliability of each system was calculated based on device unavailability related to device MTBF used in a fault tree analysis. It is obvious that the reliability of the relay and the relay Ethernet interface will dramatically affect the reliability of the RAS system. Also, the overall RAS system reliability will depend heavily on the WAN equipment. However, for the purposes of this paper, analysis was limited to the reliability of the communications systems passing peer-to-peer messages between each IED and the WAN, not including the IED, IED communications cables, or the WAN. Specifically, because the SONET equipment was common to each communications method, it was not included in the reliability calculations. Therefore, only the equipment unique to each design was compared. In other words, the reliability analysis was done comparing the different types of installations implemented over a physical SONET WAN connection. The reliability of the equipment for the physical SONET WAN was common to each design and so was not calculated into the analysis. Also, the reliability calculations are for each endpoint. Reliability of a system is the aggregate of multiple endpoints.

No reliability analysis is necessary for the system Vendor A RSRP via serial LAN because the IEDs are directly connected to one another with a serial cable. Therefore, there are no devices to buy, monitor, fail, repair, or replace.

Both the RAS protocol and GOOSE can be implemented as physical point-to-point connections by connecting two IEDs directly to one another via a dedicated channel, such as a direct fiber link. Though this is not SCE's installation preference, it does provide a more true reliability comparison between the two protocols. The use of direct fiber connections, when possible, further improves the reliability of the RAS by eliminating the SONET WAN equipment.

TABLE II
RELIABILITY ANALYSIS OF COMMUNICATIONS SYSTEM ARCHITECTURES VIA FAULT TREE ANALYSIS

Vendor	Availability	Predicted Average Annual Out-of-Service Minutes
Vendor A GOOSE Protocol via Ethernet LAN	99.982%	97
Vendor A GOOSE Protocol via Ethernet-to-WAN	99.962%	200
Other Vendor GOOSE Protocol via Ethernet LAN	99.963%	192
Other Vendor GOOSE Protocol via Ethernet-to-WAN	99.944%	295
Vendor A RSRP via Ethernet LAN	99.981%	100
Vendor A RSRP via Ethernet-to-WAN	99.961%	203
Vendor A RSRP via Serial LAN	100%	0
Vendor A RSRP via Serial-to-WAN	99.993%	37

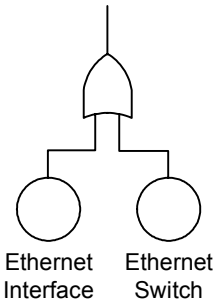

Fig. 1. Fault Tree for GOOSE Over Ethernet LAN

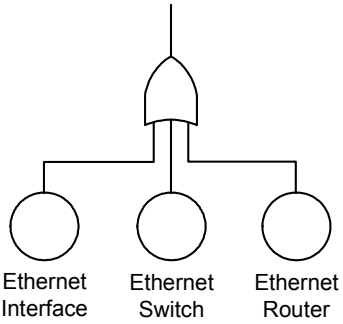

Fig. 2. Fault Tree for GOOSE Over Ethernet WAN

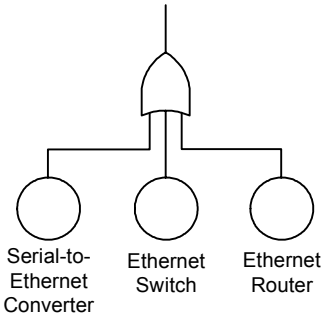

Fig. 3. Fault Tree for RSRP Over Ethernet WAN

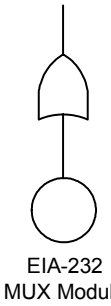

Fig. 4. Fault Tree for RSRP via EIA-232 MUX Module to WAN

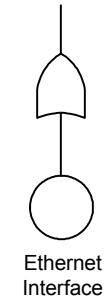

Fig. 5. Fault Tree for RSRP via Direct Fiber to Remote IED

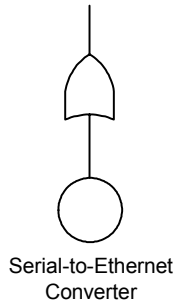

Fig. 6. Fault Tree GOOSE Protocol via Direct Fiber to Remote IED

X. System Cost Analysis

Using typical prices, the cost of each type of system was calculated for comparison. Again, for the purposes of this paper, analysis was limited to the cost of the two types of communications systems passing peer-to-peer messages between each IED and the WAN, not including the IED, IED communications cables, or the WAN. Prices are the sum of prices for the products in each fault tree illustration. The cost of equipment for the physical SONET WAN was common to each design and so it was not calculated into the analysis. Also, the cost calculations are for each endpoint. The cost of a system is the aggregate cost of multiple endpoints.

TABLE III
INITIAL EQUIPMENT COST ANALYSIS OF COMMUNICATIONS SYSTEM ARCHITECTURES

Vendor	Initial Equipment Cost(s)
Vendor A GOOSE Protocol via Ethernet LAN	$2,300
Vendor A GOOSE Protocol via Ethernet-to-WAN	$5,700
Other Vendor GOOSE Protocol via Ethernet LAN	$2,201
Other Vendor GOOSE Protocol via Ethernet-to-WAN	$5,601
Vendor A RSRP via Ethernet LAN	$1,900
Vendor A RSRP via Ethernet-to-WAN	$5,300
Vendor A RSRP via Serial LAN	$0
Vendor A RSRP via Serial-to-WAN	$450

XI. System Cryptography Analysis

Cryptographic features necessary to provide cybersecurity of the protocols associated with cyberassets include confidentiality, message integrity, and connection authentication.

As described previously, the RSRP is easily communicated over an assortment of communications systems. Due to the concise messaging and the fact that the physical and logical connections are true point-to-point, cryptography is very easily added to this protocol. Bump-in-the-wire cryptography devices quickly and inexpensively add confidentiality (via encryption) and connection authentication (via key exchange) to the messages without impacting the throughput time performance of the RAS protocol messages [5]. Integrity of the messages is assured by the physical point-to-point nature of the connections and the payload redundancy designed into the protocol.

GOOSE, as with all protocols within the IEC 61850 standard, does not have security features. A separate standard, IEC 62351, is now under development to create security methods to add to networks using this and other protocols. Therefore, Ethernet security methods are the only tools available to add cryptography to GOOSE traffic. The method available today is to segregate traffic and allow only authorized endpoints to connect to the network. The switches used are capable of grouping subsets of their ports into virtual broadcast domains isolated from each other. These domains are commonly known as virtual LANs (VLANs).

The VLAN concept is akin to other concepts in the networking world where traffic is identified by the use of a tag or label. Identification is crucial for switches to isolate ports and properly forward the traffic received. Lack of identification is sometimes a cause of insecurity and needs to be avoided [6].

As mentioned in the Questionnaire Summary section of this paper, each vendor documented support of VLAN tagging for GOOSE messages. However, it is essential that network designers choose and correctly implement switches that also support VLAN tagging for performance as well as security.

Using VLAN, GOOSE traffic authentication is provided if no other endpoints are successfully connected to the virtual network. If this is true and if a packet's VLAN identification cannot be altered after transmission from its source and is consistently preserved from end to end, then VLAN-based authentication is no less reliable than physical security. VLAN does not provide confidentiality of the messages or integrity of the contents.

XII. Conclusions

The use of RAS communications realizes significant system benefits over traditional methods of multiple copper terminations instrumenting field contacts, regardless of the protocol(s) or type of communications media used. The reduced number of field terminations, associated wiring, labor, and maintenance due to the reuse of data detected by a single IED digitally communicated to integrated IEDs and other data clients led SCE to determine the following:

- GOOSE protocol over Ethernet meets the acceptance criteria of the Ethernet RAS scheme.
- The RSRP meets the acceptance criteria of the Ethernet RAS scheme.
- GOOSE protocol is available from multiple vendors.
- The RSRP I/O module provides a successful interface to any IED for the Ethernet RAS scheme. The time is slightly slower than the acceptance criterion of 50 ms, but otherwise, it meets the acceptance criteria of the Ethernet RAS scheme and interfaces to devices from any vendor.

During testing, SCE noticed the inability to verify correct operation of the GOOSE messages on the Ethernet network unless the IEDs provided diagnostics. SCE found it essential that the IEDs provide such diagnostics to complement analysis available via network analyzers. Vendor A diagnostics provide a good example of necessary IED status and messaging status information that should be available directly from the in-service IED. This status information included:

- Message received out of sequence
- IED configuration revision mismatch detected
- IED not yet commissioned
- IED in test mode
- Message is corrupted
- Message time to live has expired
- Host disabled/not responding

Provisioning of Ethernet over SONET provides a less predictable but more efficient use of available bandwidth than the traditional provisioning of dedicated channels.

It is expected, although not proven by the research completed to date, that Ethernet provisioning over SONET will be simpler and more easily replicated than past practices. However, the same could be said for traditional channel provisioning if the same equipment was used at each site. This, however, was not a possibility for the SCE service territory.

The implementation of the RAS protocol as a point-to-point protocol closely matches the implementation of several synchrophasor protocols. Synchrophasors are becoming a very important consideration for future wide area protection and control strategies. The fact that the RAS protocol and synchrophasor protocols are implemented as point-to-point connections will simplify installations that include both protocols. This functional similarity makes the implementation, design, and troubleshooting of the combined protocols more compatible.

XIII. Appendix: SCE Vendor IEC 61850 Questionnaire

1. Do you have an IED suitable for the documented RAS that supports GOOSE?
2. Do you have an IED suitable for the documented RAS that directly supports the RSRP (Licensed Mirrored Bits)?
3. Is the IED capable of supporting RSRP via RSRP I/O modules? (This was interpreted from the responses but not asked.)
4. Does your IED have a single Ethernet port option?
5. Does your IED have two Ethernet ports with failover option where both share a single IP address and only one is active at a time?
6. Does your IED support standard engineering access via Telnet, built-in web servers, etc. on the Ethernet port?
7. Does your IED support non-IEC 61850 SCADA protocols on the Ethernet port?
8. What is the maximum number of GOOSE messages that your IED can publish?
9. Can non-Boolean data types, such as analog values, be included in your transmitted GOOSE message?
10. Does your GOOSE messaging implementation support priority tagging for optimizing latency through an Ethernet switch?
11. Does your GOOSE messaging implementation support VLAN identifiers to facilitate segregation of GOOSE traffic on the network?
12. Can you edit, configure, and change the data set transmitted in your outgoing GOOSE message?
13. Can you reconfigure your IED communications via IEC 61850 Substation Configuration Language (SCL) configuration files as specified in the standard?
14. Does your IEC configuration software read other vendor IEC 61850 SCL Configured IED Description (CID) configuration files?
15. While the IED is functioning, can the user confirm from your IED which GOOSE messages are being transmitted?

16. What is the maximum number of different GOOSE messages your IED can subscribe to and receive?
17. Can your IED use quality (q) attributes to validate individual data entries in the received GOOSE message before the data are used by your IED?
18. Does your IED monitor the health of incoming GOOSE messages?
19. While your IED is functioning, can the user confirm from the IED which GOOSE messages are being received?
20. Can your IED provide (serve) unbuffered reports?
21. Can your IED provide (serve) buffered reports?
22. Can you edit, configure, and change the data set transmitted in your outgoing reports?
23. How many client associations (IED server-to-client) are allowed by your IED?
24. Can the IEC 61850 configuration be loaded remotely (i.e., a process separate from your configuration software such as FTP)?
25. Does your IED support a command that reveals which configuration is active in your IED?

XIV. References

[1] David Dolezilek, "IEC 61850: What You Need to Know About Functionality and Practical Implementation," Proceedings of the National Convention of AEIT, Genoa, Italy, June 2004.

[2] Veselin Skendzic and Armando Guzmán, "Enhancing Power System Automation Through the Use of Real-Time Ethernet," Proceedings of the *8th Annual Western Power Delivery Automation Conference*, Spokane, WA, April 2006.

[3] Eric A. Udren and David Dolezilek, "IEC 61850: Role of Conformance Testing in Successful Integration," Proceedings of the *8th Annual Western Power Delivery Automation Conference*, Spokane, WA, April 2006.

[4] Gary W. Scheer and David Dolezilek, "Comparing the Reliability of Ethernet Network Topologies in Substation Control and Monitoring Networks," Proceedings of the *2nd Annual Western Power Delivery Automation Conference*, Spokane, WA, April 2000.

[5] Allen D. Risley and David Whitehead, "SEL-3021 Wireless Interface Security," SEL White Paper. Available: www.selinc.com/techpprs/

[6] "Virtual LAN Security Best Practices," VLAN Security White Paper. Available: www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

XV. Biographies

Mike Gugerty is a twenty-one year veteran of the Southern California Edison (SCE) Company. In his present position as part of the SCE Protection Engineering Department, he is assisting several initiatives to test and evaluate new technologies for use in wide area protection and Remedial Action Schemes. His work testing protective relays, other IEDs, and communications equipment is pivotal to verifying that new technologies satisfy SCE's acceptance criteria of speed, reliability, and cost. Gugerty has worked as a relay testman and test instructor in SCE's Transmission/Distribution Substation Training School. He has also worked as a technical specialist and test supervisor, providing technical support to SCE's Test and Automation Engineering Department.

Robin Jenkins received his BSET degree from California State University, Chico. From 1984 to 1988, he was employed as a systems integration engineer for Atkinson System Technologies. From 1988 to 1999, he was with the California Department of Water Resources, where he worked as an associate and was later promoted to a senior control system engineer. In 1999, he joined Schweitzer Engineering Laboratories, Inc. (SEL) where he currently holds the position of integration application engineer and is responsible for technical support, application assistance, and training for SEL customers in the southwestern United States.

David J. Dolezilek received his BSEE from Montana State University in 1987 and is now the Technology Director of Schweitzer Engineering Laboratories, Inc. He is an electrical engineer with management and development experience in electric power protection, integration and automation, communications, control systems, SCADA and EMS design, and implementation. He is the author of numerous technical papers and continues to research and write about innovative design and implementation affecting our 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 technical committees tasked with global standardization and security of communications networks and systems in substations.