Case Study of Mission-Critical Smart Grid Remedial Action Schemes Via Ethernet

David Dolezilek
Schweitzer Engineering Laboratories, Inc.

Presented at the
37th Annual Western Protective Relay Conference
Spokane, Washington
October 19–21, 2010

Originally published in the
proceedings of the World Energy Congress, September 2010

Case Study of Mission-Critical Smart Grid Remedial Action Schemes Via Ethernet

David Dolezilek, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—While special protection systems (SPSs) often shed load, recent sophisticated remedial action schemes (RASs) reduce or terminate generation output during an emergency condition. Under certain load conditions, generation newly added to previously balanced transmission grids creates system conditions that violate accepted reliability criteria.**

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. Testing at SCE demonstrates the successful use of IEC 61850 GOOSE (Generic Object-Oriented Substation Event) messages over a distance up to 460 miles to collect analysis and arming data and transfer status and control indications. Complete detection, alarming, calculation, and remediation are completed in well under the 50-millisecond benchmark.

Using standardized IEC 61850 GOOSE methods avoids the customization required to implement individual local RAS communications systems, allows centralized coordination of arming, disarming, and system testing, and simplifies the coordination of system maintenance. Reliability improves with capabilities to monitor end-to-end grid parameters and quickly respond to abnormal conditions.

These methods of mitigation are intended to be used throughout the SCE area of operation as well as at all interties to neighboring utilities to facilitate dynamic load shedding/generation tripping and improved load management.

SPSs and RASs must be put in place to protect existing systems that are called upon to serve new generation and load, are intertied with weak systems, or have geographical characteristics that reduce stability. Once protected, the automatic load and generation control ensures stability while improving production and reliability. Once these are in place, wide-area monitoring and control are safely added to replace state estimation with real-time state measurement and management.

I. Introduction

Contemporary special protection systems (SPSs) and remedial action scheme (RAS) systems are deployed via a network of intelligent electronic devices (IEDs) that monitor field conditions and react to contingency control actions. Protection, control, and monitoring (PCM) IEDs that are designed appropriately serve both PCM functions and monitor and control functions for RAS systems. These PCM IEDs are capable of serving both systems simultaneously; however, separate IED networks are often deployed for physical segregation. This simplifies design, installation, testing, and maintenance of PCM and RAS systems. Often, two (dual modular redundant) or three (triple modular redundant) identical IED networks are deployed to create resiliency and autonomy of the data paths and information processing. Digital communication among these IEDs is similar to that for substation automation systems (SASs) and distribution automation (DA), except that it generally travels farther to perform wide-area control. Presently, these communications travel over dedicated and deterministic channels. Recently, Ethernet and Internet Protocol (IP) methods have been used successfully for nonmission-critical SAS and even DA applications. Using very specialized products and engineering to reduce the negative impact of Ethernet bandwidth sharing methods in combination with power system-specific changes to Ethertypes, it is also possible to perform a subset of mission-critical SAS and DA applications over Ethernet. However, shared bandwidth Ethernet methods are not acceptable for any wide-area or mission-critical SAS, DA, RAS, or applications.

II. Operations Technology and Information Technology

Operations technology (OT) refers to the devices and methods, such as networks of IEDs, used to automatically control and manually operate an industrial process. In electric power systems, OT networks are specialized IED networks that include PCM IEDs and associated PCM applications. These PCM OT networks automatically control and allow manual operation of the apparatus that generate, transmit, distribute, and consume energy. The IEDs in these networks also generate, transmit, distribute, and consume information associated with the automatic control and manual operation processes.

PCM OT networks are local networks that support a substation and may also cover its neighboring distribution circuits or wide-area networks connecting several substations. For example, Fig. 1 shows several local OT networks communicating mission-critical information over a wide-area OT network. This information, including teleprotection signals, synchrophasors, supervisory control and data acquisition (SCADA) data, RAS arming data, RAS contingency alarms, and RAS mitigation control, is traditionally transported via OT network methods. Wide-area OT methods, such as time-division multiplexing (TDM), provide the deterministic and high-availability characteristics necessary for mission-critical electric power system applications.

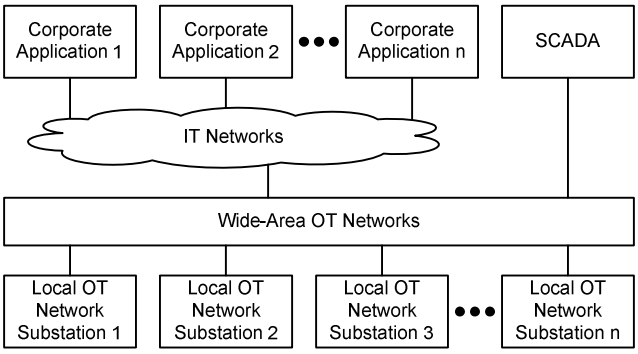

Fig. 1. Local OT Networks Communicate Mission-Critical Information Over Wide-Area OT Networks

Information technology (IT) refers to the devices and methods used to transport information among people and processes. IT networks are not the source of information, but rather the conduit to move information from the source to a remote person, process, or network. In the Fig. 1 example, IT networks provide information for corporate applications, such as planning, asset management, and billing. OT networks are the information sources for these applications. Fig. 1 shows that IT networks connect to OT networks to collect and distribute decision-making information. IT networks are represented as a cloud because their structure and behavior are variable, adaptable, and nondeterministic. These characteristics are acceptable for IT purposes where convenience and flexibility are very desirable to move smart grid information for nonmission-critical business processes.

With caution, the electric power industry has recently begun using specific, specialized applications of IT devices and methods within PCM OT networks to move data among devices and people. These devices (such as Ethernet switches) and methods (such as IP communication) are adaptable, flexible, and frequently change performance, thus the behavioral synonym and graphical icon cloud. However, the associated cloud characteristics of variability and nondeterminism created from unknown routing paths and bandwidth sharing techniques, which are acceptable in business applications, are detrimental to mission-critical applications. As mentioned, the electric power industry has created specialized Ethernet methods for a few mission-critical applications restricted to a local-area network (LAN). These methods are unique to PCM OT networks, unused by other industries, and difficult to deploy within IT devices. Specifically, many necessary changes to make Ethernet useful for electric utility OT networks have been made by IEEE and adopted by IEC. Therefore, except for a few narrowly defined applications, IT devices and methods are relegated to nonmission-critical data flow within PCM OT networks, such as engineering access and SCADA.

Present day activities focused on "smart metering" and other peripheral "smart grid" applications are being designed using bandwidth-sharing IP methods. Many activities already underway are promoting more adoption of IT technologies in local-area and wide-area PCM OT networks. However, real-time PCM applications and mission-critical communication do not exist in other industrial OT networks where IT methods have been adopted. PCM OT networks must be designed based on a clear understanding of their expected behavior. These PCM OT networks perform "smart grid actions," the activities that automate the generation, delivery, and consumption of electric energy.

As an example, consider the very different OT and IT approaches to two important PCM OT network design criteria: dependable and secure exchange of information. In this context, security is not referring to cybersecurity attributes of confidentiality, integrity, and authentication.

- *Security of communications-aided protection and control* requires deterministic latency of each message delivery. For example, security of a mission-critical control means "to refrain from tripping a breaker when not required to trip." A secure OT network is designed to guarantee deterministic, on-time delivery of each blocking or interlocking message. OT security means every message is delivered with predetermined maximum latency. IT networks are instead designed to buffer and redirect traffic to increase the likelihood that the message will eventually be delivered. IT networks optimize network throughput, meaning that the network makes a best effort to deliver each message, regardless of how long it takes. Message propagation delays of IT networks may cause protection and control problems.
- *Dependability of communications-aided protection and control* requires delivery of each message. For example, dependability of a mission-critical control means "to perform tripping when a breaker is required to trip." A dependable OT network is designed to guarantee deterministic, on-time delivery of each tripping or control message once and only once. OT network dependability means reducing lost messages to near zero. A dependable IT network is instead designed to send and resend messages to increase the likelihood that one eventually makes it through. IT dependability means the network detects and resends lost messages. Resent buffered messages of IT networks may cause protection and control problems.

Regardless of these differences, recent activities have begun to merge IT methods into wide-area PCM OT networks or replace them entirely. These include moving the IT cloud and cloud-like behavior into the wide-area OT network and local OT substation networks, illustrated in Fig. 1. IP methods of IT networks are being promoted to replace OT bandwidth reservation methods to collect data and information directly from the local PCM OT networks and distribute them for decision-making purposes. These IP methods, like other IT technology, cannot satisfy PCM OT network needs for resiliency, deterministic behavior, traffic priority, bandwidth reservation, environmentally hardened hardware, and reliability and cannot be used for wide-area communication among the local PCM OT networks. Therefore, if a single but unwittingly insufficient IP method is promoted for all grid communications, it will be able to support "smart grid information" and some, but not all, "smart grid actions." In

this case, the crucial, mission-critical protection and control "smart grid actions" in service today, which need to be further deployed to modernized the grid, will require a separate and deterministic network with near-zero message loss. Of course, the best solution is to use forethought to deploy a single smart grid communications infrastructure that performs mission-critical smart grid actions, as well as delivery of smart grid information. Fig. 2 illustrates that though IT networks are acceptable to move nonmission-critical business information, a separate wide-area OT network is still necessary for mission-critical SCADA applications.

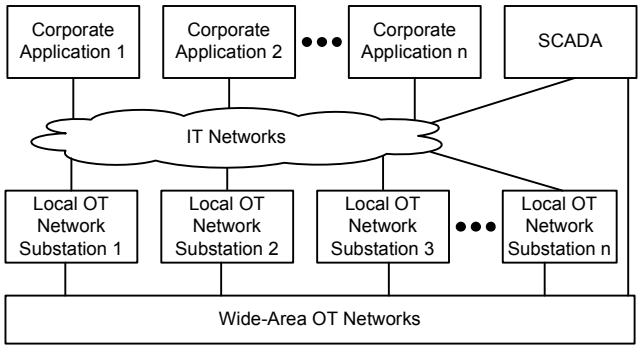

Fig. 2. Application Example of Wide-Area OT and IT Networks Connected to Substations

III. Distributed Information Processing Requires Connections Through Pipes Rather Than Packets Through Clouds

Information processing includes the results of specialized calculations within IEDs, data sharing among networked IEDs, and the processing of data to create power system information. RAS calculations require repetitive, deterministic, and reliable communication of power system measurements to prepare arming strategies. These characteristics, plus high-speed delivery, are required for messages that communicate contingency change of state (such as loss of generation) and mitigation controls (such as load shed). Wide-area PCM OT RAS networks are presently deployed using dedicated channel technologies like TDM. As the name implies, TDM technologies like synchronous optical networks (SONETs) divide and reserve the available communications bandwidth (or definitive provision capacity) into specific amounts of time to be dedicated to various applications. Each application, such as a RAS system, has a constant dedicated amount of bandwidth. The behavior synonym and graphic icon are that of a pipe. As the pipe implies, the two parts of the RAS system are connected with virtual or physical dedicated bandwidth. The application is free to use all or none of the pipe bandwidth. Unused bandwidth is dedicated to the RAS system and cannot be used by other applications. Therefore, bandwidth reservation provisioning provides deterministic, reliable communication by dedicating bandwidth to create a virtual pipe through the network. Data pipes satisfy OT network requirements of security and dependability via intentionally preventing communications interference by segregating traffic. Messages flow from source to destination while the pipe prevents multiple applications from sharing the same bandwidth. Designers are certain of the network behavior and the message path.

The IT cloud includes Ethernet and IP methods that, instead of dedicated data pipes, use data packet-based technologies because of convenience, flexibility, and multipurpose networking. Each message becomes a packet that is funneled into a multipurpose network. The network queues up and then delivers messages on a first come, first served basis. If the Ethernet switches understand the specialized electric power system message prioritization, these messages will go to the front of the queue. This process is repeated for each switch that the message passes through. Packet-based cloud networks, like Ethernet, share the available communications bandwidth (or nondefinitive provision capacity) in an ad hoc manner. Thus nonspecific amounts of time are provided to various applications as needed, and the cloud fluctuates.

When the volume of traffic increases, the message latency may increase. When the network cloud changes to reroute traffic, the message latency may increase. If a high volume of multiuse traffic causes a switch to drop a packet, the message latency definitely increases, or the message may never be delivered.

When using packet-based messaging in an OT network, the network traffic controller collects and manages the distribution of packets based on packet header information and the specific network bandwidth provisioning methods built into the system. Therefore, the in-service performance relies mostly on the engineering design and implementation and not solely on the chosen IEDs and communications technology. The network traffic controller must collect, manage, prioritize, and disperse all the packets. In Ethernet networks in which the traffic controller is an Ethernet switch, it is possible, and most likely, for IEDs to receive unwanted packets, receive packets juggled out of order, or not receive expected packets. Functionality and configuration of the network become very complicated as switch settings are manipulated and managed in an attempt to use power system-specific features.

IV. Pipes Route Messages by Design and Clouds Rely on Routing Information in Each Message

Pipe-oriented communications support both routable protocols, those with instructions to navigate a cloud in each message, and nonroutable protocols, which have no navigation instructions. The routable navigation instructions increase message overhead and create a security risk while simplifying the network engineering. The network makes its best effort to route the message through the cloud to its destination. As mentioned, the message performance will change with fluctuations in the cloud, and there is no certainty as to the route the message will take. Nonroutable messages require that the data pipes be configured in advance with a channel between the source and destination. This pre-engineering is less flexible but provides more appropriate performance and certainty of message behavior.

A routable communications protocol uses network layer address information to forward messages without knowing the path or specific receiver at the destination. Although they present several challenges to mission-critical applications, routable protocols were developed so that data could be sent among multiple Ethernet networks, intranets, and public communication such as the Internet. They allow packets to be forwarded from one network to another.

Internet routable protocols, such as Transmission Control Protocol/Internet Protocol (TCP/IP), communicate to any IP address within a LAN intranet or across the Internet. For example, a Telnet session is initiated to a network address, such as 172.168.1.1, without the need to know the specific device.

Intranet multicast protocols, such as IEC 61850 Generic Object-Oriented Substation Event (GOOSE) and Sampled Value messages, do not contain network address abilities. These protocols ignore network routing and travel to all devices in a LAN intranet unless specifically restricted, but cannot be routed outside of the LAN.

Nonroutable communications protocols contain a specific device address and, without modification, work only within proprietary LANs, such as serially connected networks or reserved bandwidth pipes. For example, regardless of the telephone number or IP address used to connect to a DNP3 device, the session is initiated only to a specific device with the corresponding DNP3 address. Nonroutable protocol messages can be routed by encapsulating them within a routable protocol, such as TCP/IP. This method is similar to call forwarding, where messages destined for a landline telephone number are forwarded to a mobile telephone number.

In summary:

- Nonroutable protocols communicate to a specific device at a specific address.
- Internet routable protocols communicate to one nonspecific device at a specific network address.
- Intranet multicast protocols communicate indiscriminately to all nonblocked network addresses on a LAN.

OT versus IT methods and nonroutable versus routable protocols play an important role in the design and performance of RAS, SPS, SAS, and DA systems.

V. RAS Using Nonroutable Protocol

The Blythe Energy Power Plant (BEPP), located in Blythe, California, was designed to incorporate a gas-fired, combined-cycle configuration consisting of two 175 MW combustion turbine generators and one 170 MW steam turbine generator. The 520-megawatt electrical output is connected to the regional transmission grid via the existing transmission system managed by the Western Area Power Administration (Western). Reference [1] describes the successful use of the Mirrored Bits® communications protocol, which is a serial peer-to-peer 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 BEPP, SCE (Southern California Edison), and around the world. It is one of the most popular nonroutable, data pipe-oriented methods within electric utility OT.

Impacts to existing power systems, typically caused by adding new generation to the established transmission grid, often include overloaded transmission lines, transformers, circuit breakers, and other system components that may cause violations of accepted reliability criteria. The North American Electric Reliability Corporation (NERC), Western Electricity Coordinating Council (WECC), and local reliability requirements determine the criteria for California installations, including the Blythe substation. To mitigate potential reliability problems, Western deployed a RAS system prior to connecting BEPP to the transmission grid. This RAS system provides generation reduction capabilities during transmission line overload conditions. Recognizing the increasing importance of having reliable RAS systems, Western chose to implement this system in a dual-primary design so that no single device or connection would be a single point of failure. Reference [1] discusses the design and implementation of these RAS systems using protective relays, communications processors, digital I/O modules, and an I/O processor.

VI. Comparing Centralized RAS Systems Using Mirrored Bits Communications and IEC 61850 GOOSE

SCE documented a case study comparing the performance of multiple communications technologies and architectures available via protection and automation IEDs for use in monitoring and controlling a RAS. The discussion includes the design description and implementation issues of several popular and standardized technologies available today to perform high-speed digital data communications among IEDs. Reference [2] describes analysis of the serial and Ethernet methods for transferring Mirrored Bits communications and IEC 61850 GOOSE messages.

A. The SCE Reasons for a New RAS Approach

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. Perhaps most important is 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 the associated RAS logic.

System reliability is expected to improve with capabilities to monitor end-to-end grid parameters and quickly respond to abnormal conditions. The mitigation area will expand from a few local choices to all nodes included within the SCE system, including dynamic load shedding/generation tripping and improved load restoration management. A new centralized

RAS (CRAS) system will mirror the success of the localized systems to a wide-area RAS that covers the SCE large service territory.

B. Design for Reliability and Decision Analysis Predict System Availability and Value

Functionally, IEDs networked together into a SAS provide operational SCADA data, engineering and analysis access, and high-speed interdevice data exchange. Reference [3] identifies the major selection and design criteria of network functionality, components, and topology. It examines and compares serial and Ethernet architectures for an example substation using the following criteria: reliability; cost of equipment and commissioning; safety; ease and cost to design, implement, maintain, and expand; effective data transfer rates; and performance of high-speed control signals.

IEC 61850-3 Section 4 states that each system shall be designed as a fail-safe design such that:

"…There shall be no single failure mode that causes the SAS to initiate an undesired control action, such as tripping or closing a circuit breaker. In addition, SAS failures shall not disable any available local metering and local control functions at the substation" [3].

IEC 61850-3 Section 4 describes the following reliability measures for design comparison:

- Reliability measured as MTBF (mean time between failures).
- Device availability measured as percent availability.
- System availability measured as percent availability.
- Device maintainability measured as MTTR (mean time to repair).
- System maintainability measured as MTTR [3].

VII. SCE RAS Message Performance Analysis

A. Speed and Control Timing

SCE established a benchmark of 50 milliseconds to detect a change, evaluate contingencies, and respond with RAS control actions in three-IED scenarios [2]. This time includes remotely detecting an abnormal condition, transmitting an alarm 460 miles over a wide-area network (WAN) to the centralized RAS controller, determining the proper actions, and then transmitting these actions 460 miles over a WAN to the appropriate remote RAS IEDs, where the control actions are implemented.

B. Test Description

The test involves three IEDs communicating to each other. IED1, the monitor IED, monitors 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, 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 hard-wired to an input on IED1. In this way, the total time duration is measured between detection of a line-open condition as a contact input on IED1 and the eventual trip output of IED3 detected as a second contact input on IED1. The time duration is measured with a separate instrument and verified with internal Sequential Events Recorder (SER) reports.

SCE staged the test with IEDs from two different vendors and tested three different protocols. IEDs from one of the vendors, referenced as Vendor A, were tested with two different protocols enabled. These tests were completed on a LAN with all IEDs directly connected peer to peer or via a local Ethernet switch and across a WAN connection via a local Ethernet switch and Ethernet router. The WAN connection was a wide-area SONET OT network. This essentially created a large LAN by connecting two remote Ethernet LANs together via a TDM data pipe over SONET. GOOSE protocol messages are published to a multicast group address and are not routable over a WAN. RAS systems and other mission-critical systems using GOOSE messages require an OT WAN to pipe the routed messages between LANs. In order to simulate in-service WAN timing for the tests, SCE used a SONET system between Los Angeles and Bakersfield, California. This was actually a data pipe that transferred data packets over a dedicated bandwidth channel and represented the furthest distance that messages would need to travel throughout the RAS system. SCE recognized that, unlike nonroutable Mirrored Bits communications, the packet-oriented GOOSE protocol installations required logical LAN connections between all RAS locations.

Fig. 3 illustrates the SCE system of PCM IED SAS networks separate from PCM IED RAS networks in the same substation. Nonmission-critical substation information may travel over IT networks; mission-critical information, including RAS and SCADA, must travel over the wide-area OT network. Bridging the two LANs in this manner over SONET raised critical security concerns that needed to be addressed separately.

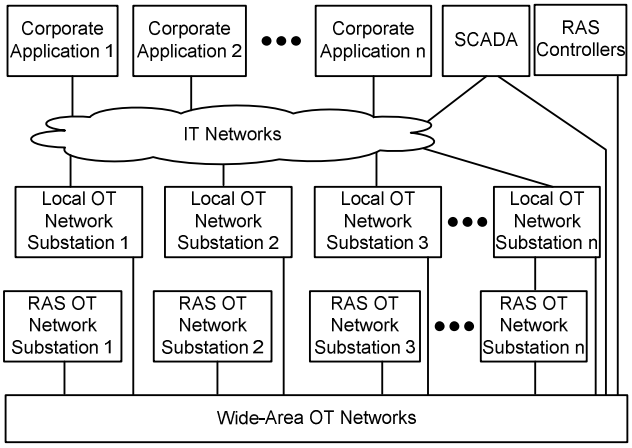

Fig. 3. Example of Wide-Area OT Connecting Autonomous RAS Substation PCM Networks Separate From IT Data Flow

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 also measured externally using a scope. The three-IED test starts with the detection of a contingency by the monitor IED, which communicates an alarm to the central IED. The central IED sends a control message to the mitigation IED, which closes an output contact. The measured duration between test start and output contact closure represents the CRAS system. Both Vendor A technologies execute in less than half of the 50-millisecond time requirement.

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

Test Case	IED Peer-to-Peer Time	Three-IED Test Scenario Peer-to-Peer-to-Peer Time
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 A MIRRORED BITS via serial LAN	4 ms	4 ms
Vendor A MIRRORED BITS via serial to WAN	9.2 ms	22.7 ms

D. System Reliability Analysis

Using fault tree analysis, SCE calculated the reliability of each system type to compare relative dependability and uptime. Table II lists the calculated expected downtime, which is a measure of unreliability due to the unavailability of the RAS system. Each time a system becomes unavailable, it also requires a substantial maintenance effort to return it to service.

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

Test Case	Availability	Predicted Average Annual Out-of-Service Minutes
Ethernet LAN	99.982%	97
Ethernet to WAN	99.962%	200
Serial LAN	100%	0
Serial to WAN	99.993%	37

The use of digital RAS communication realizes significant system benefits over traditional methods of using multiple copper terminations to measure field contact status, regardless of the protocol(s) or communications media. 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:

- The nonroutable, data pipe-oriented MIRRORED BITS communications systems meet all acceptance criteria of the CRAS system.
- The packet-oriented GOOSE protocol over Ethernet meets the performance acceptance criteria of the CRAS system.

Both GOOSE and MIRRORED BITS communications protocols are available to all vendors for purchase or license to include in their products.

VIII. REAL-TIME DIAGNOSTICS BECOME ESSENTIAL TO SUCCESS

During testing, SCE noticed an inability to verify correct operation of 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. Reference [4] illustrates diagnostics that provide necessary IED status and messaging status information directly from the in-service IED.

A. GOOSE Message Performance and Quality Monitoring

IEDs exchanging GOOSE messages automatically monitor the communications to determine message quality. Each device detects errors in received messages and the failure to receive expected messages from other devices and performs remediation immediately. The error codes indicating bad quality are summarized in Table III. If the IED detects any of these to be true, it sets the message quality to failure.

TABLE III
GOOSE MESSAGE ERROR CODES

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

B. Uniquely Identify Each Configuration Revision in the IED

IEC 61850 describes the Substation Configuration Language (SCL) and configuration files that configure devices for IEC 61850 communications. The preferred method is to load a configuration file, rather than individual settings, into the IED. Loading the file directly into the IED has several advantages over the legacy method of sending settings. A very important advantage is the ability to identify what communications behavior the IED is configured for by retrieving the filename and configuration revision directly from the IED while it is in service. Then it is possible to cross-reference the behavior of this IED and the behavior of other IEDs with the configuration files.

Further, by separating IEC 61850 configuration from other IED automation and protection settings via the SCL configuration file download, it is possible to be certain that no

other settings were accidently modified or affected. This provides security by minimizing the impact to the system, minimizing the recommissioning after a change, and eliminating the risk of unintentionally affecting the other processes within the system.

IEDs that support a GOOSE report provide real-time status of incoming and outgoing GOOSE messages and their configuration. Each report includes message configuration and performance information for each GOOSE message being published and for those to which the IED has subscribed.

Fig. 4 illustrates a GOOSE report collected directly from an in-service IED named PAC_MASTER. This report provides essential configuration parameters and diagnostics.

The GOOSE transmit status documents the configuration of the IED from which the report was retrieved. The suffix *_01* of the reference name confirms that the SCL file active in the IED is Revision 01. The multicast address, priority, virtual local-area network (VLAN), state number, sequence number, data set name, time to live, and error code are each displayed for each GOOSE message being published.

The GOOSE receive status documents the configuration of the IEDs and the associated GOOSE subscriptions configured to be received. Elements of the third subscription are highlighted to show the configuration revision and error code.

The third subscribed GOOSE message is from an IED named PAC_SLAVE_B. The suffix *_01* of the reference name for PAC_SLAVE_B confirms that the SCL file active in the IED is Revision 01. In this case, the message is not being received, and so the time to live has expired.

GOOSE Transmit Status

Reference: PAC_MASTER_01CFG/LLN0GODset14_PAC_M_DO

MultiCastAddr	Ptag:Vlan	StNum	SqNum	TTL	Code
01-0C-CD-01-00-05	4:2	367	10298	1000	

Data Set: PAC_MASTER_01CFG/LLN0$Dset14_PAC_M_DO

GOOSE Receive Status

Reference: PAC_SLAVE_A_01CFG/LLN0GODset14_PAC_A_DI

MultiCastAddr	Ptag:Vlan	StNum	SqNum	TTL	Code
01-0C-CD-01-00-01	4:2	60	18106	1198	

Data Set: PAC_SLAVE_A_01CFG /LLN0$DSet14_ PAC_A_DI

Reference: PAC_SLAVE_A_01CFG/LLN0GODset15_PAC_A_AI

MultiCastAddr	Ptag:Vlan	StNum	SqNum	TTL	Code
01-0C-CD-01-00-02	4:2	73185	5	378	

Data Set: PAC_SLAVE_A_01CFG /LLN0$Dset15_ PAC_A_AI

Reference: PAC_SLAVE_B_01CFG /LLN0GODset14_PAC_B_AI

MultiCastAddr	Ptag:Vlan	StNum	SqNum	TTL	Code
01-0C-CD-01-00-03	4:2	93732	6	0	TTL EXPIRED

Data Set: PAC_SLAVE_B_01CFG /LLN0$Dset14_ PAC_B_AI

Fig. 4. PAC_MASTER GOOSE Report Showing Transmit and Receive Configuration and Status

C. Calculate and Visualize GOOSE Message Reliability and Channel Availability

Once calculated and recorded as a time-stamped SER, each GOOSE message quality status is used to calculate reliability and availability. Message quality indicates failure when a message is corrupted or not received within the time to live. The observation of failures indicates the reliability of individual GOOSE messages. If the message quality failure is intermittent, the duration of the failures is calculated as the difference between time stamps. The aggregate of failure duration over a given amount of time determines the channel availability. Fig. 5 illustrates the use of the GOOSE quality status to alert users of a failed GOOSE subscription via the front-panel human-machine interface (HMI) to aid diagnostics and troubleshooting. In this case, a GOOSE message with analog inputs (AI) from the IED labeled *C* has failed, while the one labeled *B* is normal. It is also possible to use the status to trigger text and email messages to alert remote technicians.

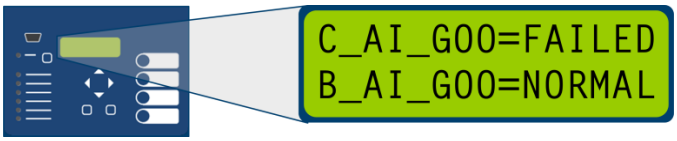

Fig. 5. PAC HMI View of GOOSE Message Quality Display Point

IX. Improving the State of the Art With Synchrophasors

To date, synchronized phasor measurements have been used mainly for power system model validation, post-event analysis, real-time display, and other similar activities. However, synchrophasors have a greater potential than monitoring and visualization. Synchrophasors will increasingly contribute to the reliable and economical operation of power systems as real-time control and protection schemes become broadly used. Synchronous phasor measurements (SPMs) are now available in relays and meters; however, a practical means of processing the data in real time has been lacking.

Reference [5] describes the synchrophasor vector processor (SVP) and several practical applications, including automated diagnostics, RAS, direct state measurement, and stability assessment. This real-time synchrophasor processor device further improves RAS and SPS systems by performing vector mathematics in real time.

A. The SVP

The purpose of the SVP is to collect SPMs, collect logical inputs, perform vector and scalar calculations, make decisions, produce outputs, and report data. A simple task for an SVP might be collecting SPMs from two ends of a transmission line, comparing the voltage angles, and issuing a warning to an operator if a threshold has been exceeded. A more complicated example might be distributed SVPs performing localized substate measurement and forwarding results to a higher level to build the entire state vector in real time, without the nonlinear and time-consuming steps of state estimation.

B. Traditional RAS System Implementation

Fig. 6 shows the timing diagram of a traditional digital communications RAS system, including the relay detection time and relay assertion output time. The system consists of approximately 73 individual pieces of equipment, including I/O modules and logic processors.

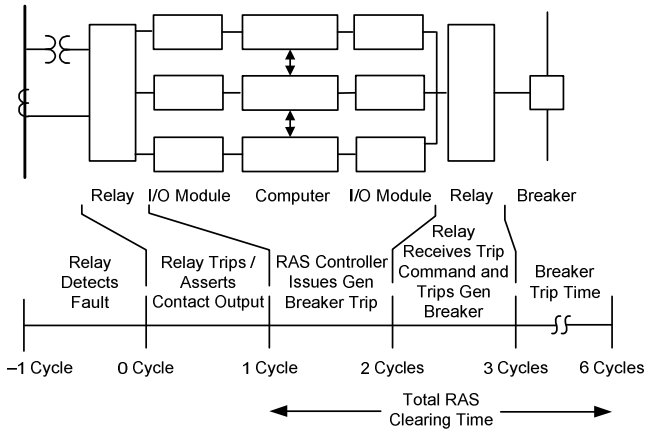

Fig. 6. RAS Clearing Time Budget

C. SVP Implementation

For the SVP RAS implementation, the relays forward synchrophasor data, and the SVP determines if there is a loss of load, overpower, etc. The net result is that implementing an SVP solution and using high-speed communications tripping can save three-quarters of a cycle.

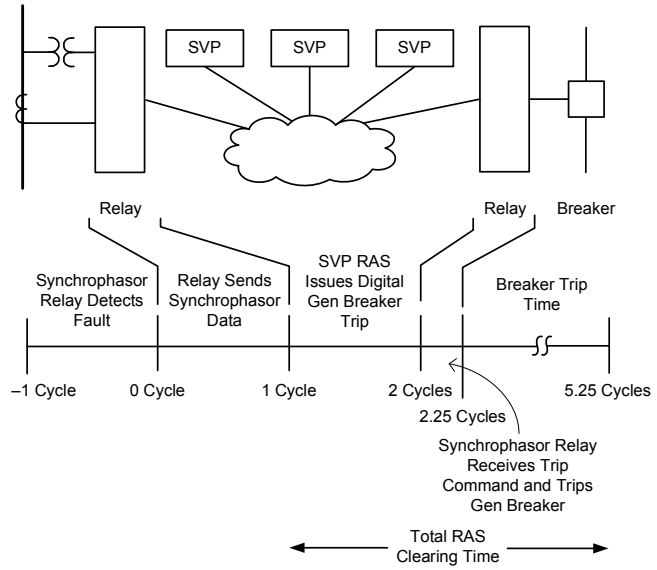

Fig. 7. SVP RAS Clearing Time

X. Conclusions

Fast and reliable RAS and SPS technologies maximize the efficiency of new and in-service generation, transmission, and distribution assets.

- Adding new generation to the transmission grid can impact the existing power system by potentially violating reliability criteria.
- Impacts to existing power systems, typically caused by adding new generation to the established transmission grid, often include overloaded transmission lines, transformers, circuit breakers, and other system components that may cause violations of accepted reliability criteria. RAS schemes are designed to rapidly acquire power system measurements and manage generation and load to prevent violations and provide stability.
- The use of digital communication for RAS data acquisition and control realizes significant system benefits over traditional methods of using multiple copper terminations to measure field contact status, regardless of the protocol(s) or communications media. The number of field terminations, associated wiring, labor, and maintenance are reduced because of the reuse of data communicated digitally.
- IEC 61850-3 Section 4 summarizes design practices and reliability measures useful to maximize system reliability and availability.
- GOOSE reports provide quick troubleshooting diagnostics by documenting configuration and status of incoming and outgoing GOOSE messages.
- Now that SPMs are broadly available from protective relays and meters, it is time to put them to work to improve the power system. The SVP makes real-time applications practical.
- Direct state measurement is now practical because of the widespread availability of SPMs. The SVP plays a role in direct state measurement and can actually reduce the amount of information communicated to the master station.

XI. References

[1] M. Agudo, D. Fox, D. Dolezilek, and R. Jenkins, "Case Study: Integrate Substation IEDs to Provide Reliable, Independent Dual-Primary Remedial Action Schemes," proceedings of the 5th Annual Power Systems Conference, Clemson, SC, March 2006.

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

[3] G. W. Scheer and D. Dolezilek, "Selecting, Designing, and Installing Modern Data Networks in Electrical Substations," proceedings of the 9th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2007.

[4] R. Jenkins and D. Dolezilek, "Case Study: Using IEC 61850 Methods for RTU Replacement and Distributed Automation," proceedings of the 10th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2008.

[5] E. O. Schweitzer, III and D. Whitehead, "Real-Time Power System Control Using Synchrophasors," proceedings of the 34th Annual Western Protective Relay Conference, Spokane, WA, October 2007.

XII. Biography

David J. Dolezilek is the technology director of Schweitzer Engineering Laboratories, Inc. He is an electrical engineer, BSEE Montana State University, with 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 our industry. Dolezilek is a patented inventor and participates in numerous working groups and technical committees. He is a member of the IEEE, IEEE Reliability Society, CIGRE working groups, and two International Electrotechnical Commission (IEC) Technical Committees tasked with global standardization and security of communications networks and systems in substations.