Integrating SCADA, Load Shedding, and High-Speed Controls on an Ethernet Network at a North American Refinery

Aboli Kulkarni
Schweitzer Engineering Laboratories, Inc.

James Payne
Valero Energy Corporation

Peter Mistretta, P.E.
Richard Design Services

This paper was presented at the 60th Annual Petroleum and Chemical Industry Technical Conference, Chicago, Illinois, September 23–25, 2013, and can be accessed at: http://dx.doi.org/10.1109/PCICon.2013.6666032.

INTEGRATING SCADA, LOAD SHEDDING, AND HIGH-SPEED CONTROLS ON AN ETHERNET NETWORK AT A NORTH AMERICAN REFINERY

Aboli Kulkarni
Member, IEEE
Schweitzer Engineering Laboratories, Inc.
10110 W Sam Houston Parkway S, Suite 130
Houston, TX 77099, USA
aboli_kulkarni@selinc.com

James Payne
Member, IEEE
Valero Energy Corporation
1801 S Gulfway Drive
Port Arthur, TX 77640, USA
Jim.Payne@valero.com

Peter Mistretta, P.E.
Member, IEEE
Richard Design Services
750 Pearl Street
Beaumont, TX 77701, USA
Peter.Mistretta@rig-rds.com

Abstract—This paper discusses the implementation of an Ethernet communications network in a ring that connects substations in a closed communications loop at a large industrial facility. Data are transmitted at protection speeds and must be dependable for industrial power system operation and maintenance applications. The redundant electric power system Ethernet communications network is used for a supervisory control and data acquisition (SCADA) system that automates industrial electric power system operations. Within individual substations as well as between substations, communications based on IEC 61850 protocols eliminate copper control wiring, which results in reduced cost, construction time, commissioning time, and wiring errors and makes future upgrades simpler. A fast load-shedding system uses the same communications network to stabilize system frequency in response to a loss of generation by detecting the events that lead to a power deficit and automatically responding by shedding load to balance generation and load in less than 40 milliseconds. This paper focuses on integrating three major electrical control systems at a refinery onto one Ethernet network: a SCADA system for controlling and monitoring operations, a peer-to-peer high-speed communications-assisted protection scheme, and a fast load-shedding system.

Index Terms—Communications network, HMI, SCADA, IEC 61850, load shedding, protection speed.

I. INTRODUCTION

A major North American refinery required integration and development of a supervisory control and data acquisition (SCADA) system. The SCADA system needed to supervise the power system, collect data from substation intelligent electronic devices (IEDs), control circuit breakers, and permit management of the power system from a central location.

The protocols within the IEC 61850 communications standard provide methods for developing best engineering practices for Ethernet-based substation protection, integration, control, monitoring, metering, and testing provided by multiple manufacturers. In this project, IEC 61850 protocols were used within individual substations to communicate with the IEDs as well as among the substations to send controls to circuit breakers. Information flows through purpose-built digital messages and communications processors or standardized protocols within the IEC 61850 communications standard, eliminating copper control wiring and resulting in reduced cost, construction time, commissioning time, and wiring errors. IEC 61850 technology also makes future system upgrades simpler [1].

Further, a load-shedding system was implemented to maintain the power system stability and survivability during any event that would cause a loss of generation to the system. In load-shedding schemes, the response time for commanding the system to recover instead of collapse is critical. In order to preserve the system, loads must be taken offline fast enough to compensate for the lost generation, maintain the system frequency, and ensure that the effects of the event are mitigated.

All the tasks related to SCADA, communications-assisted protection, and fast load-shedding require a very robust, reliable, and safe communications network. This paper focuses on the implementation of an Ethernet-based IEC 61850 network for these critical systems.

II. COMMUNICATIONS ARCHITECTURE

With a continually increasing amount of information available to engineers and management, a modern industrial facility requires an information and communications technology (ICT) communications network for collecting electrical data from devices in the field, sending controls to remotely located IEDs, providing engineering access, and downloading event records and equipment operational reports from IEDs. Various options were considered for the communications network at the refinery, including serial and Ethernet networks. A disadvantage of a serial-based network provided by multiple manufacturers, given the multiple communications functions required, is multiple connections and cables to the same IED. Standard protocol serial connections are limited to a fixed bandwidth and a single protocol. Combining all of these functions into one single communications medium would be a significant decrease in the number of communications links required. This can be done with a group of purpose-built protocols multiplexed over a serial cable or packet-based Ethernet protocols. Because only one manufacturer provides these purpose-built protocols, an Ethernet-based network provides this flexibility for solutions involving multiple manufacturers [2]. Recent improvements to Ethernet communications hardware, such as industrialized network switches, have both improved the reliability and decreased the cost of implementing an Ethernet network in an industrial facility. Ethernet networks are flexible and are implemented using copper, fiber, or wireless physical connections. These networks support various protocols such as DNP3, Modbus® TCP/IP, IEC 61850 Manufacturing Message Specification (MMS), IEC 61850 Generic Object-Oriented Substation Event (GOOSE), and IEC 61850 Sampled Values (SVs), as well as many proprietary protocols. Due to these advantages, an Ethernet-based network was used in designing the communications architecture. Fig. 1 shows the system architecture diagram.

Modern Ethernet local-area networks (LANs) are physically implemented in a star, ring, or linear topology or some combination of those topologies. There are multiple advantages and disadvantages to each of these topologies, but an in-depth discussion of each network topology is out of the scope of this paper [3]. The long-term goal for this project was to implement a high-speed load-shedding system with high network availability, so a ring topology wide-area network (WAN) with LANs in star topologies was implemented. A ring topology network requires two outgoing communications cables from each point on the ring and is a single-fault tolerant network, meaning it has the ability to survive a single point of failure or a device being turned off on the ring. Fiber-optic cabling covers long distances and offers simple cabling. The network availability is less than that of a redundant star topology network, but it is considered acceptable and is possible at a greatly reduced cost.

Another concern was network latency, which is the time between the source sending a packet and the destination receiving it. Ring topology network latency is slightly higher than that of a star topology, but it is not significant in this relatively small network.

Managed Ethernet switches are intelligent devices that allow data to be directed to the appropriate device based on Internet Protocol (IP) addresses or multicasting, which makes the communications network more efficient. Ethernet switches create the backbone of the Ethernet network and control the capacity and speed of the network. Managed Ethernet switches provide many benefits in a communications network, including the following:

1. Virtual LANs (VLANs). Support for IEEE 802.1Q allows the use of VLAN capabilities [4]. VLANs allow the IEDs to send multicast messages directly to the desired receivers. The Ethernet switches are configured to use VLAN information in the IED multicast GOOSE message to make virtual connections to a few IEDs, even though they are physically connected to all IEDs in the LAN. Also, if the network has logical groups of devices that are different from the physical groups, such as cameras and telephones separate from IEDs, then a VLAN-based switch is required for traffic optimization. IEEE 802.1p provides message prioritization so that higher-importance control messages can be processed before lower-importance information messages [5].
2. Rapid Spanning Tree Protocol (RSTP). RSTP is a switch communications protocol that allows the managed switches to optimize and configure the direction of traffic flow throughout the communications network.

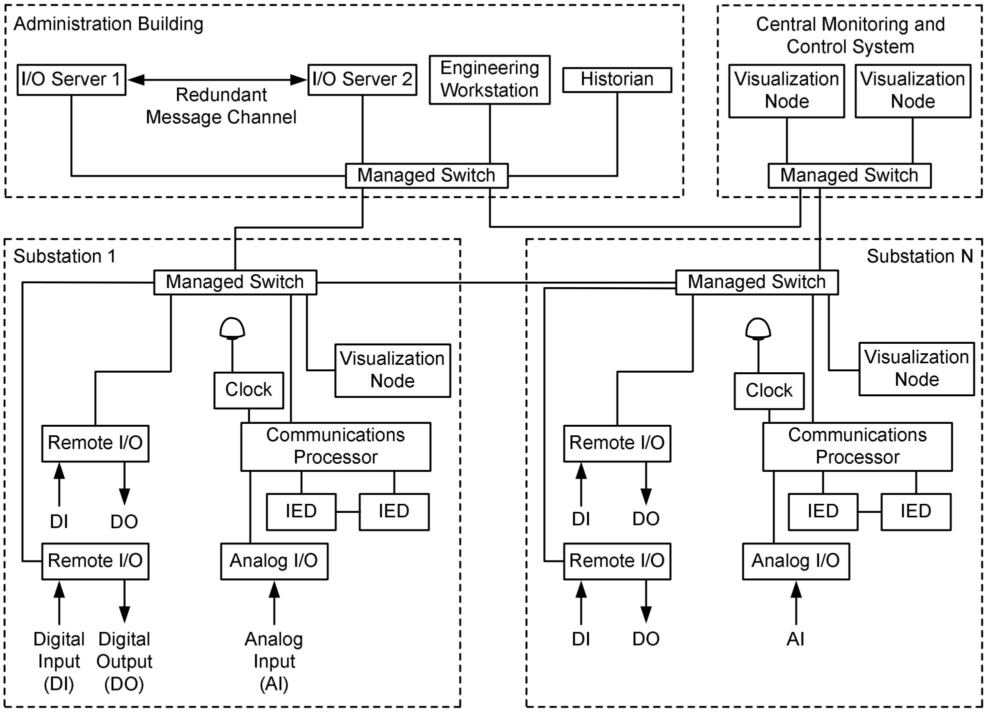

Fig. 1 System Architecture

Table I shows various LAN technologies that are used in the industry for Ethernet networks. Based on the maximum distance and data rate, IEEE 802.3 [6], IEEE 802.3u [7], and IEEE 802.3z [8] were chosen for the communications network in the refinery.

TABLE I
LAN TECHNOLOGY SPECIFICATIONS

Name	IEEE Standard	Data Rate	Ethernet Connection Type	Maximum Distance
Ethernet	IEEE 802.3	10 Mbps	10BASE-T	100 m
Fast Ethernet	IEEE 802.3u	100 Mbps	100BASE-TX 100BASE-FX	100 m 2,000 m
Gigabit Ethernet	IEEE 802.3z	1,000 Mbps	1000BASE-T 1000BASE-SX 1000BASE-LX	100 m 275 to 550 m 550 to 5,000 m

III. SCADA SYSTEM IMPLEMENTATION

Implementing a SCADA system into an older refinery presented several challenges. The existing IEDs were from multiple manufacturers and communicated on various protocols, often over a serial network. A method of controlling the circuit breakers and interfacing with all IEDs needed to be developed. Additionally, many substations were decades old and presented arc-flash hazards during circuit breaker operation. The ability to control these circuit breakers from a safe location, even if the SCADA system was nonfunctional, was desired. Additionally, because the network would be shared with communications-based protection systems and a high-speed load-shedding system, network traffic needed to be minimized.

A SCADA system model with a central server was selected. This allowed for a common graphics package to be developed for each substation so that all human-machine interface (HMI) screens are available at any HMI view node. This design allows for minimal updates anytime changes are implemented. Redundant I/O servers allow for increased uptime and system availability, and a central historian server provides easy access to event records and trending data from any view node. Additionally, network storage is supplied to allow for network backups and software implementation.

A. Communications Processor

At each substation, a communications processor was installed to provide translation from serial to Ethernet. The communications processor, which is used to collect data from the IEDs and provide control functions, allows for connections to the IEDs either serially or through Ethernet and supports various protocols via protocol conversion. The communications processor collects the data from devices from various manufacturers. It collects the IED analog metering data, target elements, and I/O statuses and offers data manipulation, concentration, and processing capabilities. The communications processor can scale analog data to the appropriate values and units for display on SCADA, and the data can be used to calculate average currents and voltages. The communications status of each IED is monitored to check whether the IED is offline or online. Boolean logic is used to display the IED status. The communications processor concentrates the data for transmission to the SCADA I/O servers to minimize network traffic and latency [9].

Redundant I/O servers are used to collect data from the communications processors and send these data to SCADA software. The primary I/O server does the main polling and updates the HMI screens. If the primary server fails, the backup server starts polling the data and updates the HMI screens. Once the primary server is restored, the backup server returns to an idle mode.

The network storage is used to keep a central repository of all IED settings in the refinery, which greatly reduces errors related to previous poor IED settings record management.

B. Substation Remote I/O

Many of the existing substations at the refinery did not allow for remote control of the devices over the network. Remote digital I/O devices were installed at each substation to provide the SCADA system with the ability to open and close circuit breakers, raise and lower transformer taps, and provide 52A, 52B, and truck-operated contact (TOC) statuses back to the SCADA system. With the long-term goal of providing load shedding throughout the refinery, the selected remote I/O devices provide Ethernet and IEC 61850 capabilities to allow for operation outside of the SCADA system [9].

C. Engineering Access

The communications processors provide engineering access to each connected substation IED via an innovative pass-through feature at the same time as ongoing data acquisition via serial multiplexing. Users access the IEDs and view the event files, energy reports, and load profile reports, as well as view the settings and make any necessary changes to the settings remotely without interrupting data flow to the SCADA system [9].

D. Time Synchronization

One of the main issues the refinery electrical staff faced was analyzing faults and failures with data from unsynchronized time clocks. The SCADA system has satellite time clocks at each substation so event records can be time-stamped with accurate Global Positioning System-based (GPS-based) time to improve future fault analysis. The communications processors act as network time servers and distribute time synchronization to all devices on the network. Thus the IEDs and their data records are synchronized to a common time, even if the IEDs are not capable of accepting IRIG-B time synchronization directly. Demodulated IRIG-B has an average accuracy of ±100 nanoseconds.

E. Security

The SCADA system requires multilevel passwords to protect access. Each user has specific assigned roles and has access to the system based on those roles. The IED network uses defense-in-depth strategies, where each level (IED, data aggregation, and LAN communication) has password and access security, as well as digital and physical alarm outputs for both expected and unexpected connections.

F. SCADA Software

The SCADA system was designed with a software package that has helped to ensure future upgrade capability and compatibility. Fig. 2 shows a typical one-line operator view. Using standard software packages simplified the training of refinery staff to use and support the system [10].

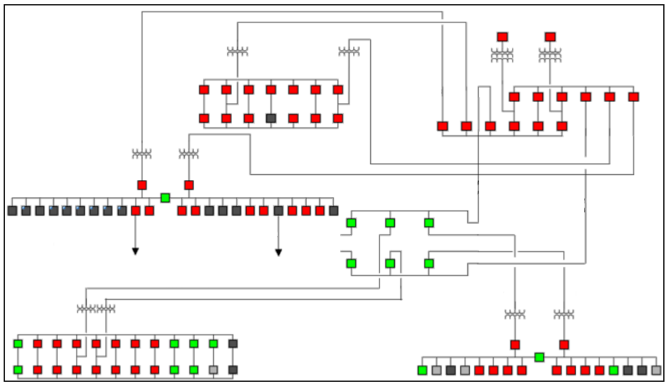

Fig. 2 One-Line Diagram Screen

In addition to the primary SCADA system, each substation has a local HMI, which is a part of the communications processor and is used to monitor and control the system from the substation. These HMIs also serve as a backup SCADA system if the primary SCADA system is down.

G. Alarms, Historical Alarms, and Trending

The SCADA system collects and collates system-wide alarms from the substation IEDs. Alarms are logged so that the user can view past alarms at any time to diagnose or analyze one or more events that occurred on the system. Alarms are listed chronologically by the time of day or relative to a particular chosen event under analysis.

Sequential Events Recorder (SER) reports are extremely useful for quickly reviewing a timing sequence. The time and date stamps of event reports are synchronized to an IRIG-B time source input. IED time stamps are accurate to the millisecond, and the accuracy remains associated with the data change record stored in the IED as well as when data are passed to the SCADA system. This feature is useful when analyzing and coordinating event reports from different IEDs within the same substation and the events from IEDs located at different substations. Trending helps to view the change in the analog values at a specific time and helps analyze the cause of the faults on the system.

IV. SUBSTATION CONTROL USING IEC 61850

Each substation that is part of the electrical power system network of the refinery has a managed Ethernet switch to facilitate the ring communications formation. These switches are connected through Ethernet cabling (fiber and copper) to the various IEDs and SCADA equipment in a star or hub-and-spoke topology within the substation. These interconnected IEDs perform the necessary data acquisition and control to form the SCADA system. In new substations, IEDs will be selected that directly support Ethernet connectivity. In this fashion, SCADA control is executed via digital messages over Ethernet using IEC 61850 commands. It logically follows that the protection communication from IED to IED is done through this same network. IEC 61850 GOOSE messages are used to send state information, interlocks, direct trip indications, blocking signals, and/or measured analog values. This results in the elimination of large quantities of copper interconnect wiring that was previously used to transmit this information electronically [11]. This wire reduction has many benefits, including the following:

1. Lower cost due to less wiring time and material.
2. Reduced commissioning time due to fewer physical connections and easily repeatable logic checks.
3. Higher reliability due to the inherent fault checking and supervision capability of digital communications. This is true for serial- and Ethernet-based peer-to-peer messaging.
4. Reduced (though not eliminated) engineering, moving from the manual craft labor of instrumentation wiring and manual paper documentation to software-based engineering design and automatic electronic documentation.

An existing eight-bay double-breaker double-bus 230/69 kV substation was upgraded, and the Ethernet network was used to transfer information as well as controls. The only copper wiring necessary in this installation was for the current transformer (CT) and the voltage transformer (VT) wiring to IED terminals. However, because this was the first implementation of IEC 61850 GOOSE, optional dual primary signals were also installed via copper conductors.

A. Intrasubstation Communications Architecture

One of the many appropriate design concerns with an Ethernet network for protection and control in a substation is the failure of a network switch or other component. The entire purpose of substation ICT networks is to manage or mitigate malfunctions in the power system. If the necessary message is unable to be delivered, the malfunction can escalate into a catastrophe. It is the role of engineers to understand and mitigate the known and predictable failure modes of the ICT network as well as perform due diligence design to reduce the negative impact of unexpected failures. Failure to observe communications errors in an Ethernet network must not be confused with the absence of communications errors. Due to the nature of Ethernet, communications actions are not always clear. Therefore, engineers designing mission-critical ICT networks must learn, understand, and use the first principles of Ethernet messaging and network design [2] [3]. Also, if a communications failure does occur and nothing catastrophic happens, this is not an indication of system resiliency. It is an indication that, by chance, the mitigation operation and network outage did not overlap and the outage should be investigated to find root cause.

Known and predictable failure modes of Ethernet networks include network unavailability due to the following:

1. Bandwidth saturation when a link or port receives more data packets than it can buffer and send.
2. Data path reconfiguration via RSTP or another protocol. Modern Ethernet configuration forbids more than one active path at a time, so redundant cables do not provide redundant communications, and failover takes various amounts of time. IEEE 802.1aq (Amendment 20: Shortest Path Bridging) will address this failure mode.
3. Firmware upgrades that take the switch and all associated data flow out of service.
4. Cyberintrusion that consumes switch and IED communications resources even if the attack does not successfully compromise the device.
5. Physical failure of a power supply, port, or cable.

Manufacturers have responded to these concerns by offering IEDs with redundant Ethernet ports and messaging based on IEEE 802.1 and ISO/IEC 15802-1 multicast addressing [12], IEEE 802.1Q VLANs, and IEEE 802.1p prioritization, among other technologies. The Ethernet ports are configured as either switched ports or failover ports.

Using the ultra-high-reliability hub-and-spoke design for direct connections between the communications processor and the IEDs, the intrasubstation communications at the refinery were designed to be able to operate completely independent of Ethernet switches, if necessary.

As shown in Fig. 3, one high-speed protection (primary) IED, an overcurrent protection (backup) IED, and two redundant circuit breaker monitoring and control IEDs (A and B) located in the circuit breaker cabinet in the switchyard are used to protect one breaker bay. The circuit breaker monitoring and control IEDs convert the received IEC 61850 trip and close indications into actual output voltage signals and convert and publish the voltage input signals as IEC 61850 status indications.

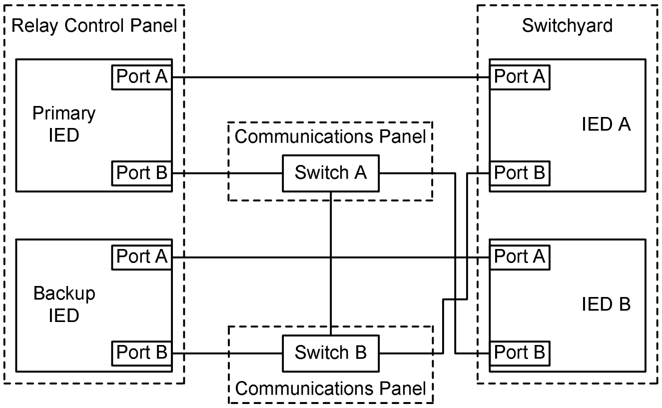

Fig. 3 Communications Architecture

The Ethernet ports on the primary IED are configured as failover ports, with the primary port going to the circuit breaker control IED A and the backup port going to the substation managed Switch A. The Ethernet ports on the backup IED are also configured as failover ports, with the primary port going to the circuit breaker control IED B and the backup port going to the substation managed Switch B. The ports on the circuit breaker control IED A are configured as switched ports, with one port connected to the primary IED and the other port connected to the substation managed Switch B. The ports on circuit breaker control IED B are also configured as switched ports, with one port connected to the backup IED and the other port connected to the substation managed Switch A. The resulting communications architecture created by this scheme is completely $n - 1$ redundant and not dependent on any one managed switch, fiber or copper Ethernet cable, or IED.

B. Overcoming the Nondeterministic Nature of GOOSE Messaging

Another engineering design concern with GOOSE messaging is the fact that it is transported via multicast Ethernet packets. All Ethernet technology is nondeterministic because it must use various methods with unforeseeable results to share the bandwidth among all the applications using it. This requires extensive network engineering and appropriate Ethernet switches to reduce jitter to acceptably low values. Also, because there is no acknowledgement of GOOSE messages, the publisher cannot determine if published messages reach their destination. This becomes an issue when dealing with a time differential protection scheme such as breaker failure. Breaker failure protection begins timing from the instant a trip command is issued and continues timing until the fault current disappears. To accomplish this type of protection scheme, two other features are used in this protection application: GOOSE message quality and slow breaker detection.

The circuit breakers used in this particular installation are 3-cycle breakers. The circuit breaker control IEDs are programmed to begin timing upon receipt of a GOOSE trip signal. The initiating primary IED subscribes to field signals via a GOOSE message from the circuit breaker control IED A. This repetitive GOOSE exchange acts as a virtual wire between the two IEDs, transmitting the present status and current measurements from the field. All subscribing IEDs constantly calculate the health of incoming GOOSE messages and use this calculation to supervise the communications link. If for any reason the GOOSE exchange fails, the message quality fails and is set to true. This status is used directly in the subscribing IED to supervise and modify the logic so that the logic knows that the communication failed, and the logic reacts right away. If the breaker does not open and GOOSE messages are being published but the breaker status remains unchanged, the primary IED is able to differentiate healthy GOOSE messages with unchanged breaker positions from silence due to a communications failure. The IED waits 3 cycles for the breaker to open. If the breaker does not open within 3 cycles, the circuit breaker control IED A calculates a slow breaker alarm and sends a corresponding signal in a slow breaker GOOSE message back to the trip initiator [11] [13]. This serves the following three purposes:

1. The IED performing breaker failure timing now knows that the breaker has definitely received a trip signal, the breaker has applied voltage to the trip coils, and nothing has happened for 3 cycles.
2. The GOOSE exchange is supervised, and any failures are recorded in the subscribing IED SER.
3. If the circuit breaker does eventually open before the breaker failure protection operates, an alarm can be sent to indicate that a circuit breaker is not performing as it should and maintenance should be performed.

C. Communications Health Real-Time Monitoring

The bus differential IED in the substation needs to be able to communicate with every IED in the substation due to the nature of the protection scheme. This makes the bus differential IED the perfect candidate to perform real-time communications health monitoring. Should any of the IEDs within the substation lose communication, stop communicating to the bus differential IED, or go into an alarm condition due to self-testing, the bus differential IED detects it and sends an alarm. Any network failures among the other IEDs not detectable by the centralized bus differential IED are calculated in each subscribing IED. These failures are combined and reported to the SCADA system to inform operations that the electrical network has lost some sort of electrical protection or digital communications.

V. LOAD SHEDDING

The refinery had historically operated with balanced generation and load and only tied to the local utility for backup purposes. Recent expansions at the refinery elevated the load, which caused a significant generation deficiency, making the utility tie necessary for operations. A load-shedding scheme was required to maintain the power system stability and industrial system survivability in case of separation.

Power system stability can be maintained if the correct amount of load is tripped offline fast enough when an event occurs on the power system. Specific events require mitigation of appropriate loads to sufficiently reduce the impact of the disturbance on the power system so that it remains stable. Industrial system survivability requires that individual loads be quickly and intelligently selected to minimize the loads lost in a load-shedding situation. A flexible, intelligent load-shedding system must only shed loads that are not mission-critical and only the amount required to balance against available generation.

The load-shedding system requires process-intense logic to control the fast operation when a generation deficit occurs, particularly when the industrial system is islanded. A slow response while shedding load can lead to cascading outages and cause a complete system blackout. The load-shedding scheme was designed based on the following two criteria:

1. Shed load as fast as possible and avoiding a frequency drop below a level where the industrial system cannot be recovered.
2. Selectively shed loads instantly based on the operators periodically changing priority schedules.

Based on these criteria, contingency-based load shedding was selected as the primary scheme. An underfrequency load-shedding scheme based on underfrequency IED settings is used as a backup scheme.

The refinery has two 230 kV utility tie sources and four on-site generators. The system network is shown in Fig. 4. The two utility tie sources and two generators are connected to two 230/69 kV substations, each with a double-breaker double-bus arrangement on the 69 kV side. The two 69 kV substations supply power to 13.8 kV substations for plant distribution. Two generators feed the 13.8 kV substations.

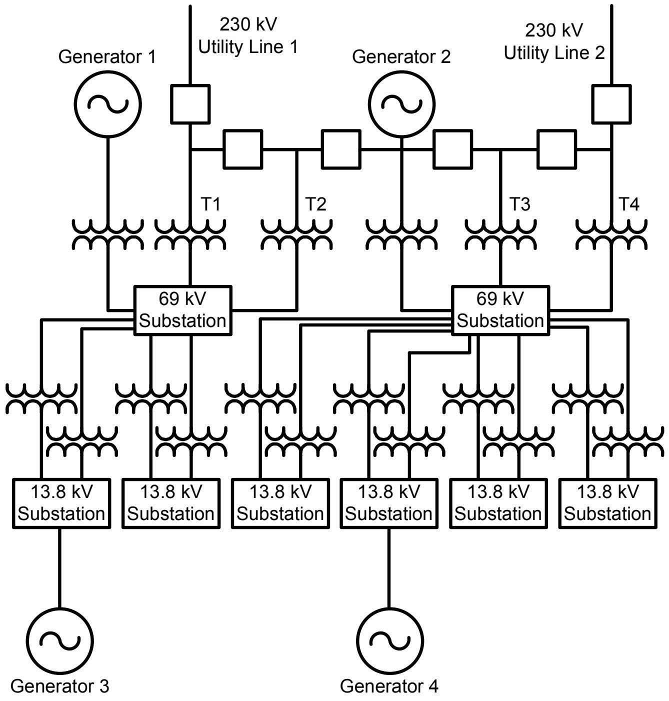

Fig. 4 Electrical Power System Network

A. Contingency-Based Load Shedding

The primary load-shedding system dynamically calculates the amount of load to be shed based on each predetermined contingency and selects loads based on the operator-settable priorities that consider system topology, real-time load mitigation, and power deficit in the power system [14]. These selections are frequently calculated and incorporated into the system so that shedding reacts immediately rather than taking time to calculate selections during an event.

1) *Conceptual Architecture*

Conceptually, the load-shedding system is divided into two functional categories: pre-event calculations and event actions. The system performs pre-event calculations to dynamically determine which load to shed and to update a load-shedding table. The system monitors contingency triggers and generates load-shedding signals. Fig. 5 illustrates the conceptual architecture [14].

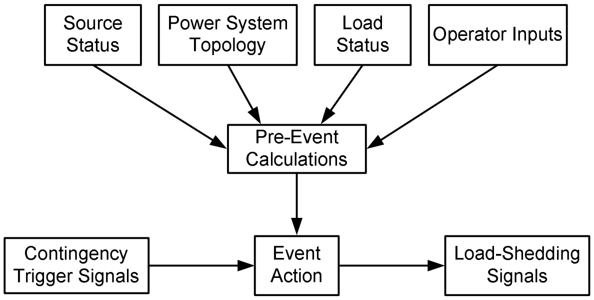

Fig. 5 Conceptual Architecture

2) *Physical Architecture*

Front-end processors (FEPs) relieve the load-shedding processors (LSPs) of the process-intensive task of communication with IEDs at the substation level. The FEPs are used to concentrate the IED data without burdening the LSPs and then send the data to the LSPs. Fig. 6 illustrates the physical architecture of the load-shedding system.

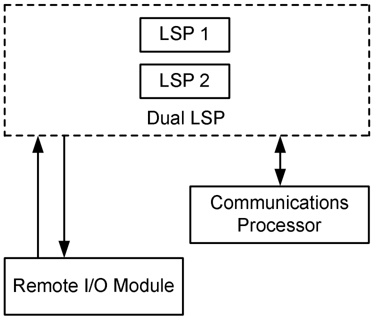

Fig. 6 Physical Architecture

3) *Load-Shedding Contingencies*

The load-shedding system responds to the loss of a generator, transformer, or tie-line or bus-tie breaker opening. These conditions are initiated by the change of state of breakers, trip signals, or lockout IED operations representing the state of the primary equipment. The primary equipment for contingency-initiated load shedding in this system includes the following:

1. Two utility lines (when system is islanded)
2. Four generators
3. One tie line
4. Four transformers

Islanding is detected by a combination of breaker openings, and the subsequently required amount of load is shed in the islanded region based on the system topology.

A crosspoint switch configuration was implemented to allow for reconfiguration of the priorities and responses to a contingency event. A crosspoint switch is a two-dimensional matrix that aligns each potential contingency with a set of mitigating outputs. This allows flexible and frequent changes in priorities, removal of loads from the load-shedding pool, and changes to contingencies while still maintaining constant arming of the system for immediate action.

4) *Dynamic Load Selection*

The load-shedding system performs process-intensive tasks to calculate the amount of load to be shed and selects the loads based on the priority for each contingency that can occur. Fig. 7 shows the algorithm that the LSPs perform every 2 seconds [14]. These results are constantly updated to the crosspoint switch to arm the scheme.

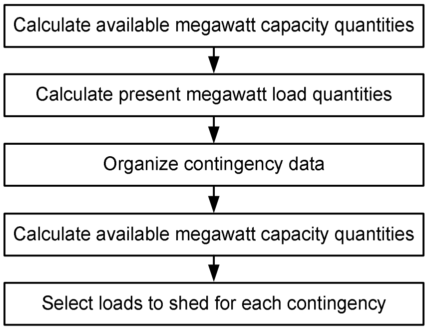

Fig. 7 Load Selection Algorithm

B. *Backup Underfrequency Load-Shedding Scheme*

The backup secondary load-shedding scheme is based on underfrequency thresholds. The underfrequency threshold values are decided based on the detailed model developed for the refinery power system. The data from the manufacturers are used for modeling different power system components such as generators, transformers, transmission lines, distribution lines, and cable. The model was tested to fine-tune the values to determine the underfrequency pickup and time-delay settings used to initiate underfrequency contingencies [15]. The frequency is measured from the IED with direct VT connections, which monitor the sheddable loads. If the system frequency falls below a threshold, loads are shed with the help of underfrequency protection pickup signals in the IEDs. This underfrequency scheme dynamically selects loads from operator-configurable load priorities and balances the generation to load. The scheme provides for three levels of underfrequency (UF) set points, as shown in Table II.

TABLE II
FREQUENCY SETTINGS

Setting	UF Level 1	UF Level 2	UF Level 3
Frequency pickup	59.5 Hz	59.2 Hz	58.9 HZ
Pickup timer	7 cycles	7 cycles	7 cycles
Megawatts to shed	1 to 40 MW	1 to 80 MW	1 to 120 MW

The algorithm for underfrequency load shedding also uses the crosspoint switch. This provides load-shedding reaction times similar to the contingency-based load shedding. The IED at each sheddable load sends the frequency value to the FEPs, which process the data and send the data to the LSPs. The LSPs use the operator-set frequency pickups, pickup timers, and real-time megawatts to calculate load-shedding set points.

As a third solution, the underfrequency protection in the IEDs will act independently to shed or trip in order to protect primary equipment in the event that the LSP primary contingency and backup underfrequency algorithms both fail to operate correctly.

C. Load-Shedding Timing

The load-shedding scheme must be fast enough to maintain power system stability. High-speed performance of the load-shedding scheme is achieved through the use of the LSPs, fiber-optic cabling, and the IEC 61850 GOOSE protocol.

The LSPs are used to perform all of the processing necessary to detect the contingency trigger signals from remote I/O modules or IEDs via the FEP, perform logic functions, and send out load-shedding signals according to the present contents of the crosspoint switch via digital messages to the FEP. The FEP then sends the load trip signal through the Ethernet network using IEC 61850 GOOSE messages for high-speed tripping.

The speed at which a load-shedding event action occurs depends on the following delays:

1. Input and output processing in the remote I/O modules.
2. Program execution time of the LSPs and FEPs.

The LSPs execute the high-speed crosspoint programs every 2 milliseconds. Table III summarizes the total roundtrip delay times and total load-shedding trip time. Table IV shows the total load-shedding trip time that includes the breaker opening time delay.

TABLE III
LOAD-SHEDDING EVENT DELAY TIMES

Action	Delay (ms)
Input debounce	2
IEC 61850 GOOSE message latency (IED to FEP)	<5
FEP processing and update	<4
LSP update	4
Communications update (LSP to FEP)	<4
IEC 61850 GOOSE message latency (FEP to IED)	<5
Contact close	6
Total	<30

TABLE IV
TOTAL LOAD-SHEDDING TRIP TIMES

Action	Delay (ms)
Total roundtrip time	30
Breaker opening time delay	50
Total load-shedding trip time	80

VI. CONCLUSION

By implementing an ICT communications network, the refinery was able to increase the flexibility of the electrical protection and control systems. Improvements to Ethernet hardware have made Ethernet a reliable, rugged, and inexpensive method for providing information to SCADA systems, performing peer-to-peer protection and interlocking, and issuing controls using IEC 61850 protocols. The Ethernet network also provides for the easy implementation of future expansion and scheme changes and the infrastructure for a redundant load-shedding scheme for a refinery.

The contingency-based load-shedding scheme was implemented as a primary scheme with an underfrequency-based load-shedding scheme as a secure secondary backup in the event that the primary scheme fails. The Ethernet network contingency-based load-shedding scheme was tested, and the results show that the scheme operates in less than 30 milliseconds.

Engineers have an obligation to understand and mitigate known and predictable failure modes of Ethernet and design resilient systems to mitigate an unexpected failure. Failure to observe communications errors in an Ethernet network must not be confused with their absence. Though data exchange engineering is not eliminated, it is reduced and moved from the manual craft labor of instrumentation wiring and manual paper documentation to software-based engineering design and automatic electronic documentation.

Careful product selection and Ethernet network design in this system provide a modern ICT system that is available, dependable, and secure. In turn, it is used to create a remedial action and protection system that is dependable (operating each time expected) and secure (prohibiting unwanted operation) in order to maintain stability and provide survivability.

VII. REFERENCES

[1] S. Kimura, A. Rotta, R. Abboud, R. Moraes, E. Zanirato, and J. Bahia, “Applying IEC 61850 to Real Life: Modernization Project for 30 Electrical Substations,” proceedings of the 10th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2008.

[2] P. Talacci, S. Dey, and R. Moore, “Applying an Ethernet LAN in a Substation,” proceedings of the 7th Annual Western Power Delivery Automation Conference, Spokane, WA, May 2005.

[3] G. Scheer, "Comparison of Fiber-Optic Star and Ring Topologies for Electric Power Substation Communications," proceedings of the 1st Annual Western Power Delivery Automation Conference, Spokane, WA, April 1999.

[4] IEEE Standard 802.1Q-2011, IEEE Standard for Local and Metropolitan Area Networks – Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks.

[5] IEEE Standard 802.1D, IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Bridges.

[6] IEEE Standard 802.3, Standard for Information Technology-Specific Requirements.

[7] IEEE Standard 802.3u-1995, IEEE Standards for Local and Metropolitan Area Networks: Supplement to Carrier Sense Multiple Access With Collision Detection (CSMA/CD) and Physical Layer Specifications Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units, and Repeater for 100 Mb/s Operation, Type 100BASE-T.

[8] IEEE Standard 802.3z-1998, Gigabit Ethernet Standard.

[9] R. Jenkins, D. Dolezilek, D. Darms, and B. Gurney, "Case Study: Efficiently Replace PLC Automation Systems by Integrating IEDs With Fiber-Optic and Ethernet Communications in the Substation," proceedings of the 5th Annual Power Systems Conference, Clemson, SC, March 2006.

[10] D. Dolezilek, K. Carson, K. Leech, and K. Streett, "Secure SCADA and Engineering Access Communications: A Case Study of Private and Public Communication Link Security," proceedings of the 5th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2003.

[11] N. Seeley, "Automation at Protection Speeds: IEC 61850 GOOSE Messaging as a Reliable, High-Speed Alternative to Serial Communications," proceedings of the 10th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2008.

[12] ISO/IEC 15802-1995, Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Common Specifications.

[13] 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.

[14] W. Allen and T. Lee, "Flexible High-Speed Load Shedding Using a Crosspoint Switch," proceedings of the 32nd Annual Western Protective Relay Conference, Spokane, WA, October 2005.

[15] B. Cho, H. Kim, M. Almulla, and N. Seeley, "The Application of a Redundant Load-Shedding System for Islanded Power Plants," proceedings of the 35th Annual Western Protective Relay Conference, Spokane, WA, October 2008.

VIII. VITAE

Aboli Kulkarni received her master's degree in electrical engineering from Tennessee Technological University in 2010. After graduation, Aboli joined Schweitzer Engineering Laboratories, Inc. as an electric power automation engineer in Houston, Texas. She has been involved in the development, design, implementation, and commissioning of automation projects. She has experience in the field of power system automation.

James Payne is an electrical engineer at the Valero Energy Corporation Port Arthur Refinery. His focus is on distribution and relay protection. James began his career as an electrical engineer at Dow Chemical in 1999. He joined Eaton Electrical in switchgear sales in 2000. He earned his BSEE from New Mexico State University in 1998.

Peter Mistretta P.E., is an electrical engineer for Richard Design Services. His career began at Dashiell Corporation in 2008 as an electrical design engineer. His focus is on electrical system studies and protective relays. He earned his BSEE from Louisiana State University in 2008.

Previously presented at the 60th Annual Petroleum and Chemical
Industry Technical Conference, Chicago, IL, September 2013.

20130430 • TP6582