The Application of IEC® 61850 to Replace Auxiliary Devices Including Lockout Relays

Robert Brantley METC, LLC; **Kevin Donahoe P.E.** GE Energy; **Jacobus Theron** GE Multilin; **Eric Udren** KEMA T&D Consulting

Introduction

The Michigan Electric Transmission Company (METC) serves the bulk of the Michigan Lower Peninsula outside of the Detroit region. METC was incorporated in 2002 and owns the 345 kV and 138 kV bulk power transmission system comprising 82 substations and over 5400 miles of interconnecting transmission lines.

METC needed to address the declining performance, unreliability, and increasing operating and maintenance (O&M) costs of legacy protection and control systems. In general, the reliability trend of METC's protection and control systems has been stable, but the overall cost to repair malfunctioning relays is increasing. About 63% of existing relays were installed prior to 1980. While age is not a direct driver of poor reliability of relays, there is an ever-increasing trend of failed relays or increased maintenance of relay components due to the effect of out of specification parts on performance. Also, many specific classes of older relay designs and generations are experiencing rapidly increasing age-related deterioration and failure. Many of these relays lack technical performance features that are important for secure operation of the system under today's increased loading and stresses. This population of relays consists largely of electromechanical (EM) and first generation solid state relays for which the pool of technically capable service technicians is dwindling. METC currently has only about 12 percent penetration of microprocessor relays.

Faced with this aging population of relays and substation control equipment, METC established a programmatic approach to perform a wholesale upgrade of the entire protection and control system in all substations in an aggressive multi-year program. METC developed key supplier partnerships that integrate and implement the entire scope of the project. METC's partners interact closely with the METC in-house project management team, bringing specialized technical expertise where needed and taking responsibility for successful implementation results.

In 2004, to begin the process, METC and its partners conducted an assessment of existing protective relaying and substation control systems. This was followed by development of a forward-looking technical strategy for the replacement program. METC and its assessment partner, KEMA, created the strategy based on METC business needs, the industry regulatory and system reliability situation, and assessment of available technology. The upgrade strategy focuses on:

- Creating goals and a far-reaching roadmap for protection and substation automation design.
- Evaluating advanced technology available in the time frame of the upgrade project.
- Integrating protection and control to develop and distribute information to help with all aspects of METC business and operations. Both operational and non-operational data flows are critical to success.
- Utilizing the features of new devices and systems to reduce the amount of equipment, floor space, and hardware failures while improving protection performance.
- Reducing and ultimately eliminating time-based maintenance while improving availability, security, and dependability.
- Foreseeing and defining issues for managing new relays, systems, and data gathering features.
- Developing a benefit-cost analysis (BCA) to justify investment in a complete upgrade program.
- Learning lessons from recent experiences, and resolving specific METC and industry performance issues in the upgrade design.
- Specific implementation approach for the new strategy.

With economic justification from the BCA, and a program of powerful business and technical advantages defined in a new strategy, METC selected a vendor team comprising GE* Multilin*, GE Energy, IBM® for business integration and data information management; SBC (now AT&T) for communications infrastructure, and KEMA for technical support on protection, control, design, testing, and utility operating needs. During 2005, METC and its project team have been developing the design for the new protection and control buildings, as well as the communications infrastructure and back-office business applications to yield information for all categories of enterprise users from the masses of substation data.

Technical Strategy

METC settled on a technical strategy that uses features of new substation LAN technology to directly achieve METC goals. The strategy is based on systems of equipment in commercial service or successful pilot installations elsewhere. However, the design emphasizes innovative ways to combine the proven functions and elements, building on what has been demonstrated to achieve greater operating and cost benefits. High-level objectives are:

- Improved network security.
- Greatly reduced quantity of equipment, wiring, and space.
- Reduced installation and operating cost.
- Rapid status, equipment performance, and event situation reports.
- Equipment condition data to prioritize major capital investments.

The upgrade design uses an integrated architecture for substation automation (SA) and protective relaying. The new scheme has these key features:

- Relays and other intelligent electronic devices (IEDs) communicate via local area networks (LANs) for operational integration.
- SCADA, EMS, and substation human-machine interface (HMI) all operate from the same shared data streams on the LANs.
- Relays, IEDs, and databases are integrated with the corporate WAN for non-operational substation information access throughout the enterprise.
- The strategy integrates a new generation of multifunctional microprocessor relays in two (not more) highly isolated equivalent and redundant subgroups with improved relaying.
- Equipment monitoring IEDs evaluate and communicate operating data for major capital equipment.

Technical Architecture Benefits

METC will achieve the following major benefits with the new architecture:

Economic:

- Reduce the number of relaying panels and zones by better than 50%.
- Reduce the quantity of equipment and panel space by better than 75%.
- LAN data sharing cuts redundant wiring of signals by better than 50%.
- Completely eliminates SCADA remote terminal units (RTUs), stand-alone digital fault recorders (DFRs), and sequence of event recorders (SERs).
- Control over the redundant high-speed LANs eliminates masses of critical control wiring and switches, while adding self-diagnostic capability.
- Equipment condition monitoring (ECM) IEDs give data to extend life of capital equipment and defer or prioritize replacement expenses.

Reliability:

- Focuses and improves performance of protective relaying, using new measurement functions and elements.

- Gives a path to gradually eliminate Zone 3 relays, handling the power-system events that Zone 3 intends to cover by adding new redundancy and communications.
- Eliminates Zone 3 limitations on line loading where Zone 3 is still used.
- Relay communications and overlapping self-monitoring catches and alarms relay and system malfunctions before they cause system trouble.

Operating:

- The central substation HMI replaces manual controls and metering now spread over all the control house panels.
- Reduces amount of equipment to track and maintain.
- Reduces and eventually eliminates routine on-site testing and calibration.
- Gives fast access to time-synchronized fault and disturbance data for analysis and restoration of system failures.

The recommended strategy meets NERC design standards in effect at time of design and directly addresses current concerns regarding how relaying functions in system emergencies. The strategy also corrects or eliminates the causes of minor relay misbehavior incidents observed in recent METC operating experience.

Architecture Overview and Features

Figure 1 shows a simplified overview of the protection and control architecture for a 345 kV control house. Note these features of the design:

1. All of the protective relays, and most of the other substation IEDs, are able to connect directly to an Ethernet LAN using optical fibers.
2. The LAN serves for data gathering, control, and protective communications among the relays. Dedicated control wiring, panel controls, and lockout switches are eliminated.
3. All relays and associated LANs are segregated into two (not more) highly isolated and fully redundant systems. The functions in the two sets are completely duplicated.
4. For 345 kV bulk transmission, there are two physically separated batteries and charging systems, feeding physically separated relays with isolated wiring and fiber runs.

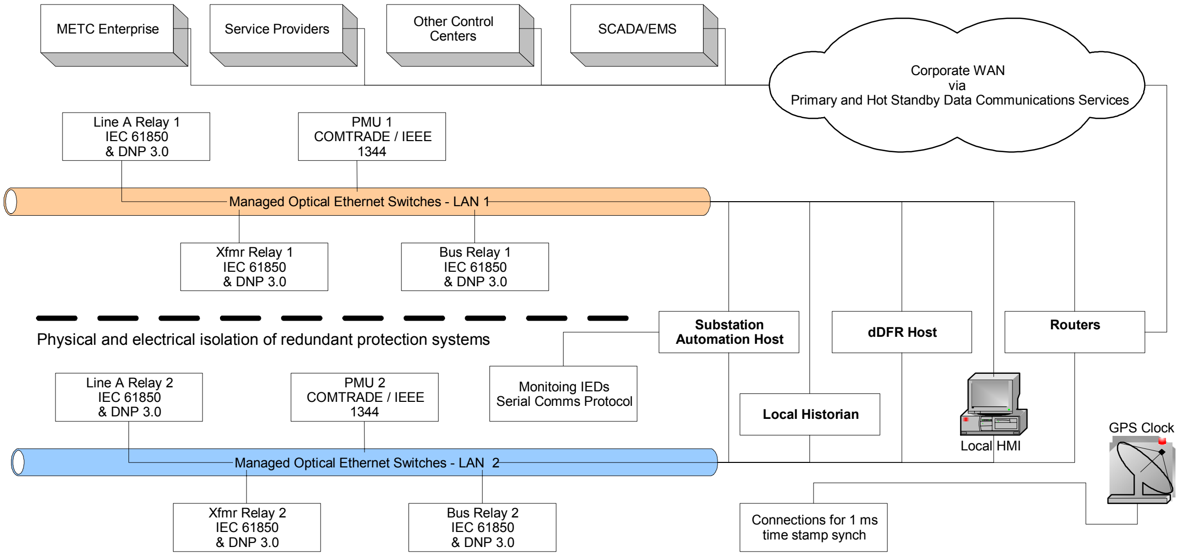

METC Enterprise
Service Providers
Other Control Centers
SCADA/EMS
Corporate WAN via Primary and Hot Standby Data Communications Services
Line A Relay 1 IEC 61850 & DNP 3.0
PMU 1 COMTRADE / IEEE 1344
Managed Optical Ethernet Switches - LAN 1
Xfmr Relay 1 IEC 61850 & DNP 3.0
Bus Relay 1 IEC 61850 & DNP 3.0
Physical and electrical isolation of redundant protection systems
Substation Automation Host
dDFR Host
Routers
Line A Relay 2 IEC 61850 & DNP 3.0
PMU 2 COMTRADE / IEEE 1344
Monitoing IEDs Serial Comms Protocol
Local Historian
Local HMI
GPS Clock
Managed Optical Ethernet Switches - LAN 2
Xfmr Relay 2 IEC 61850 & DNP 3.0
Bus Relay 2 IEC 61850 & DNP 3.0
Connections for 1 ms time stamp synch

Figure 1 New Substation Protection and Control LAN Architecture

5. Communications for pilot line protection and transfer tripping for backup protection are also separated, isolated, and duplicated.
6. The design is arranged so that no credible single failure impacts both protection systems.
7. The IEDs at the power system interface level include fault recording, swing recording, and phasor measurement (PMU) functions.
8. IEDs on the redundant LANs provide a connection point for contact and analog I/O that is not associated with a particular zone of protection.
9. The user interface computer provides local control via a one-line display on a monitor with control and data screens. The user interface computer is backed up by manual control buttons and text displays on the relay front panels.
10. A local SA host computer or concentrator performs the functions of a traditional RTU, including programmable logic and interface to multiple control centers. It gathers power system data and performs control via communications with IEDs on either or both redundant LAN segments, rather than by separated connections and measurements found in the legacy RTUs.
11. The SA Host and Historian can also deliver data through the WAN to data hosting centers and to enterprise.
12. A notably important information serving function is the delivery of complete system monitoring data for the power equipment and for the protection and control system. Not only the IEDs, but their auxiliary systems and interconnections, are monitored and the results are accessible to a remote maintenance team. The maintenance can be handled by METC, or by a service provider at another location working under contract.
13. Fault and swing recordings are served directly over the LANs and WAN to local substation or remote personnel who need to analyze details of disturbances, faults, and equipment operations.
14. The system is designed to support phasor measurement data serving to meet the strategy being carried out by the US Department of Energy's Eastern Interconnection Phasor Project (EIPP).
15. Coordinated substation and control center Historian systems retain a track record of substation actions and information that is robust in the face of WAN communications outages.
16. Routing devices at the WAN interface include communications management, and perimeter cyber security as required in NERC® CIP standards.
17. Serial IEDs, such as transformer gas-in-oil monitors and a weather station, connect directly to the SA Host, which serves this information to other systems and users.
18. GPS based time synchronization signals connect to all timekeeping IEDs to achieve 1 ms coordinated time tagging.

Using the LANs

The dual redundant protection LANs combine to provide a network communications path to substation level devices – the SA host, the user interface, and the historian, among others. There is also a routed and secured connection to the WAN. Both primary and hot-standby backup wide-area connections are provided for critical operational data.

Despite widespread belief to the contrary, note that multiple Ethernet-based protocols can be combined on one LAN to achieve all the required functions. The METC approach favors the use of IEC 61850 substation control communications [1] wherever practical. While IEC 61850 is the emerging industry standard, products will continue to appear over several years until a full suite is available. Meanwhile, effective systems can be created that mix 61850 communications with established Ethernet-based protocols. These include Ethernet DNP3 and Ethernet Modbus® (Modbus TCP). Specific server and client devices exchange data using the message format they both understand. The Ethernet LAN infrastructure, including fibers, data packet switches, and packet routers, all handle the mixed protocol traffic with no challenges.

Use of IEC 61850 GOOSE Messaging

The architecture uses the IEC 61850-8-1 GOOSE messaging on the LAN for communications among relays, to eliminate wired connections. GOOSE messages are used to transmit breaker trip commands from one relay to others that actually connect to those breakers. They also convey lockout commands, breaker failure initiation, and reclosing initiation. GOOSE messaging on the redundant LANs combines with logic in the relays and station-level computing units to implement overall control and lockout, eliminating relay panel wiring and switches. Each field point connects to only one relay or IED.

A notable virtue of GOOSE messaging is that it carries on continuously, transmitting either analog values or status information with time tags to any receiving relay on the LAN. The receiving relays look for this constant message stream, and can report instantly if the stream is no longer received or if messages are occasionally absent when expected. A stream of do-not-trip messages comprises a very responsive monitoring function for a rarely used tripping connection, and receiving relays alarm instantly if the message stream goes away. The failure can be corrected right away. Note that conventional wiring and lockout switches cannot achieve this active monitoring.

Overview of IEC 61850 and GOOSE Messaging

IEC 61850 Overall

IEC 61850 [1], *Communication Networks And Systems In Substations*, includes a broad range of services and tools for monitoring, control, and protective relaying. From the outset, the standard has been architected to describe power system application objects that can be transmitted over widely used, evolving and advancing layers of data communications technology. With this approach, years of development work for substation automation and protection object modeling can be mapped to new communications systems as they evolve. So utility users can take advantage of the rapid advancement of IT LAN and WAN technology for the indefinite future, without discarding the old protocol work and starting over again.

Power system objects in 61850 comprise measurement values from relays or IEDs, status of binary points within those IEDs, and control objects that convey action commands to those IEDs. Part 7 of 61850 describes the object modeling approach, the abstract communications services interface (ACSI) to standard communications layers, specific object definitions and descriptions, and logical node and data classification in which these objects are arranged.

A key feature of 61850 IEDs is that they are able to describe themselves – what objects they have available to serve or can receive - to higher-level systems. This feature enables a connection of relays and IEDs to be set up for LAN communications very quickly, compared to the manual process of manually defining and entering a points list as is done with preceding substation control protocols. Part 6 of 61850 also defines a substation configuration language (SCL) to be used in software tools that make it easy for users of the 61850 relays and IEDs to set up the interunit communications according to the substation connection topology, and the functions needed for protection and control.

Parts 8 and 9 of 61850 comprise specific communications services mappings (SCSMs) – how the substation and power-system objects and their organizational structure are to be communicated using standard communications layers that are in widespread and growing use without regard to utility or substation applications. In theory, the power system objects could be mapped and communicated over almost any well-defined, stack oriented communications system.

Part 8 is focused on communications over the substation bus, which is the LAN integrating the relays and control house IEDs, corresponding to the two LANs in Figure 1. Part 9 focuses on communications services for the process bus, which is a LAN connection to switchyard or power apparatus sources of the raw process information – high-speed streaming of instantaneous voltage and current sampled values, equipment status reports, and access to control circuits of breakers, switches, and other equipment. For the current discussion, we focus on Part 8. The process bus, Part 9, is in an earlier phase of development by the industry, and is an application of future interest to METC and many other utilities.

While Part 8 could include mappings to a variety of LAN environments (including those that have not been invented yet), Part 8-1 that is now in the Standard focuses on mapping of substation objects to an

Ethernet LAN, with TCP/IP or certain other protocol layers, and the ISO®-standard application layer called Manufacturing Message Specification (MMS) developed for industrial process control.

Readers interested in more details on IEC 61850 Station Bus and Process Bus protocol and architecture can conveniently refer to [1], presented at the present conference, and references it lists. For the present purpose, we focus in on the high-speed multicast messaging objects for control, Generic Object Oriented Substation Event (GOOSE) messages, whose capabilities allow protection and control system designers to turn the familiar protection panel design approaches upside down.

GOOSE Messaging Operation

Most of the information or control messages in 61850, DNP3, or other protocols are single transmissions of snapshot values or requests. By contrast, GOOSE messages are designed to convey an effectively continuous indication of the state of some logic or control point, or analog value. If control wiring is to be replaced with control messaging, this continuous indication of state is key. There are many functions in relaying, such as the output state of a relay (picked up or dropped out), which can change at any instant. Other parts of the protection scheme need to know about these state or value changes in real time. A dedicated wire handles this job; the GOOSE messaging service has to be able to accomplish the same thing using a LAN connection that is shared with so many other messages and services.

Readers may see references in other papers to either GOOSE or GSSE messaging. The latter is also part of IEC 61850, and performs the same function as GOOSE messaging. IEC 61850 GSSE messaging can convey binary states and control requests, but not analog values. It is the 61850 implementation of what was called GOOSE messaging in the forbear UCA™ LAN control design, and was ported into 61850 as GSSE messaging for compatibility with existing UCA designs.

Publisher-Subscriber Model

To begin, the GOOSE message is not addressed by the sender to a particular receiving relay. Rather, it is sent as a broadcast (actually multicast) message that goes onto the LAN with identification of who the sender is, and with the identification of the specific message so that its point contents can be determined by listeners. There is no destination address. Every other relay and IED on the LAN can see the message, and decide on its own whether it needs to look at the contents of this message.

The transmitting IED is called the *publisher*, and any other relay or IED that is configured to look for and use this particular message is called a *subscriber*. IEC 61850 provides for convenient setup of publisher-subscriber relationships based on self-description by potential publishers, and automatic configuration tools mentioned in the last section. In early implementations by vendors of GOOSE messaging, the automatic configuration may not be available; but if the message publication and subscription is set up manually by the user (with relay settings), the messages on the LAN are genuine GOOSE messages that are fully compliant with IEC 61850 specifications. This also means that relays from multiple vendors can all subscribe to and properly interpret a GOOSE message from a particular brand of publishing relay.

GOOSE messaging is also an unconfirmed service. This means that the publisher has no mechanism for finding out if all the subscribers got the latest information – in fact, it does not even know who all the subscribers are. There is no mechanism, and really no time, for a long list of subscribers to come back and confirm that they got the message, nor can they request a retransmission. Because of this, the publisher must keep on filling the LAN with updated GOOSE messages, and the burden of catching them falls to the individual subscribers.

Streaming Transmission of States or Values

In protection schemes, the contact state or analog value transfer from one relay to another may need to be updated in real time at least every few milliseconds to work correctly. So a single message isn't adequate. In GOOSE messaging, each publisher sends its state or value messages over and over again,

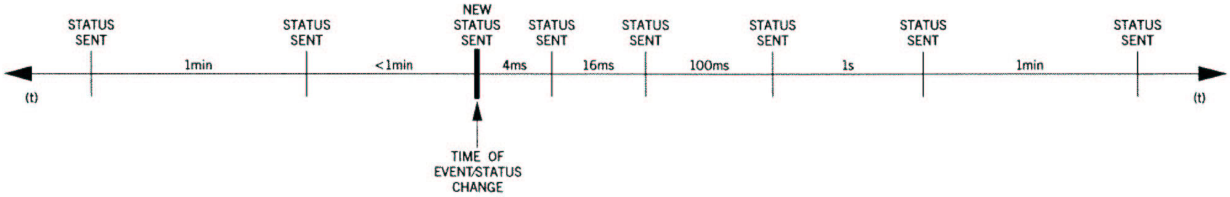


Figure 2 Adaptive transmission time interval of GOOSE messages

often enough to keep all the subscribers up to date. The actual rate of message publication is adaptive, depending on whether the transmitted states or values are changing.

Figure 2 illustrates the message repeat intervals as implemented. Note that a particular published GOOSE message may contain multiple signal states. If all of the states are stable (no status change; analog values within a set deadband), the particular message is published with the relatively long time interval of 1 minute. If *any* state or value in this published message changes, the updated message is transmitted with no intentional time delay. Also, the *time between transmissions* drops to lower values, adequate to keep the subscribers updated on the latest state for relaying purposes as the fault or power system situation continues. After the power system application stabilizes again, the GOOSE message logic in the publishing relay notices that states are not changing any more, and returns to stable state rate of message transmission. In Figure 2, the intervals increase between messages as the protection functions on the LAN settle back to their normal quiescent states. If any change suddenly occurs during this throttling-back situation, the time between messages shifts back down.

This logic for controlling the rate of transmission is implemented entirely in the publishing relay or IED for a particular GOOSE message. All the subscribers must be capable of recognizing, capturing, and interpreting the stream of these messages at whatever rate the publisher chooses to send them.

Steady-State Low-Rate Message Transmission

The reader may now wonder why the messages are constantly republished, even at a low rate, when the power system is running smoothly and nothing in the message is changing. There are three key reasons:

- If any subscriber relay fails, is turned off, is replaced, or loses contact with the LAN, it will eventually come to life again. When it does, it must be able to determine quickly the state of GOOSE values to which it was subscribed. There is no mechanism for it to request and update. The burden is on the publisher to insure that all the subscribers are aware of the states of message content at all times.
- If any publisher relay fails or loses contact with the LAN, all the subscribers will find themselves lacking the periodic updates (and they all will likely alarm for the failure). When the publisher comes back to life, it needs to look at its application inputs, and begin the steady-state transmission sequence to get all the subscribers back up to date. It will generally do this by starting out using the shortest retransmission time, and then throttling back to the lower rate used for stable conditions. All the subscriber alarms will reset.
- The reception by a subscriber of the stream of GOOSE messages it is programmed to watch comprises a critical self-monitoring function for the LAN control capability. It gives the user the ability to know at all times that the application microprocessor – the mind – of the publisher relay is able to send critical control messages to the application processor – the mind – of each of the subscribers. If expected messages disappear at any subscriber, the subscriber alarms for maintenance attention.

This last point is one of the most powerful drivers for use of GOOSE control. Users always know when a control path fails, and we don’t have to wait for an incorrectly relayed fault to find this out. This continuous monitoring of the ability of control links to work is something that wires and lockout switches were never capable of doing. While those wires and switches were quite reliable, it was also impractical to test them often, even manually. We can now replace faith in the integrity of wires with constant confirmation of the integrity of LAN control. And we can repair failures when they occur, before a fault and operating problem points out the failure to us.

Performance Requirements for Relays and the Ethernet LAN During Faults

In IEC 61850 and the forbear UCA™ LAN control applications, it is required that the control message transfers occur within 4 ms. As a practical matter, more demanding new applications and newer LAN capabilities are expected to lead to even shorter control message times, and the LAN can handle the faster messaging. The designer of a relay must architect the hardware and software so as not to add undue delays to detection of power system states and the relay's timely generation of updated GOOSE messages. Also, the relay must be able to recognize, decode, and act on subscribed messages fast enough to meet the application requirements.

Note that a particular relay can be (and generally is) both a publisher and subscriber for GOOSE messages. So the designers have to make sure that it can implement both the transmission logic we just described for each published message, and also can catch and decode all the messages to which this relay is subscribed. There is no mechanism for synchronizing the messages flying around among relays – each has to deal with the stream as it arises in a real fault situation. Multi-zone or evolving faults with breaker failures or other problems can produce a storm of GOOSE messages flying among relays on the LAN. Standards committee working groups have spent effort to make sure that a typical Ethernet LAN would not be overwhelmed [2]. A typical modern LAN can indeed handle the message rate for such a busy moment, and in fact the LAN technology is advancing so rapidly that the margin of safety grows dramatically by the year.

It is beyond the scope of this paper to explain the detailed operation of the LAN components and equipment, such as the relay Ethernet ports, or the Ethernet message-packet switches that are used to interconnect all the relays with optical fiber Ethernet links (see Figure 1). However, it is worth pointing out here that the use of modern Ethernet switches eliminates all possibility of packet collisions that characterized earlier-generation Ethernet LANs. The switch can queue, organize, and prioritize the flow of messages among all the networked relays and IEDs, so that no messages ever collide or get lost. For GOOSE messages, newer switches can recognize a priority value in the message frame and push a critical GOOSE message to the head of a transmission queue, jumping ahead of lower-priority traffic like oscillographic data file transfers or metered-value readings for SCADA.

We emphasize that the Ethernet LAN and its message packet switches are now performing critical protective relaying functions. Accordingly, it is wise to use switches now available that are hardened for substation use – tested to withstand the physical and electrical environments that the relays themselves have to withstand. IEEE® Standard 1613-2003 [3] has been published to define these environmental withstand requirements for networking components that perform relaying jobs.

As the application of Ethernet LANs propagates in new protective relaying designs, relay engineers and technicians will need to become familiar with the functioning, behavior, and characteristics of Ethernet switches and other protection system components.

Applying GOOSE Messaging in Control Schemes

In the new substation design this paper describes, GOOSE messaging is used to replace wiring and panel switches for critical protection. Examples of functions GOOSE messaging can be used for include:

1. Breaker trip messages – from a relay that wants to trip a breaker, to a different relay to which that breaker trip circuit is actually connected.
2. Breaker close messages – same situation.
3. Relay or logic output states for supervision of protection or control actions in other relays or zones of protection.

4. Breaker failure initiation
5. Reclosing initiation
6. Transfer of reclosing control – when two redundant sets of relays protect a line, only one can be in charge of automatic reclosing. The relay normally in charge transfers reclosing control to the backup relay only if it is out of service. The two relays use a protocol of exchanged messages to establish which is alive, and which is in charge of reclosing for the line.
7. Cross monitoring of redundant relaying systems – each can check for life in the other system, and report failures, without any additional wiring.
8. Backup trip commands, following breaker failure or backup relay operation.
9. Breaker lockout and close blocking commands
10. Breaker lockout states – indication that a particular lockout is in effect for a particular breaker.
11. Maintenance tagging lockouts
12. Maintenance testing state or control-inhibit state for LAN messaging – inhibit normal response by subscribers.

Eliminating Conventional Wiring and Controls

The introduction explained METC's objective of cutting cost, panel and floor space, and complexity of wiring, and ongoing maintenance testing costs in the new P&C design.

We note that, with GOOSE messaging ability and with programming of logic in the publishing and subscribing relays, we can *completely eliminate* the panel wiring, control switches, and lockout switches used for apparatus control. This is a key objective in the present METC upgrade project. Figure 3 shows one example of the wiring that will be replaced. In the original design to lockout the transformer, the PRI relay tripped three auxiliary relays each referred to as PRIX. Between all four relays five breakers were tripped, the close circuits for all five breakers were disabled, alarms were initiated and an input to the events recorder was provided. To perform these functions the design presented requires no additional wiring beyond that shown in Figure 1 and connections from an IED to the trip coils of each circuit breaker.

Primary control and management of the power apparatus is carried out through the HMI of a substation control computer, shown in Figure 4, which gets its view of the power system situation from the substation data concentrator, and in turn from the relays and other IEDs.

For backup to this substation computer and HMI, the individual relays have pushbuttons, LEDs, and alphanumeric text display for breaker and function states, breaker controls, lockout management, metered values, event reporting, and maintenance, as shown in Figure 10. No panel space, wiring, or controls are used for these functions.

Not using GOOSE messaging, but also critical in the wiring elimination, is the abandonment of a conventional separately wired digital fault recorders (DFRs) or sequence-of-event recorders (SERs). In the new design, event and oscillographic data recording over a variety of fault, disturbance, and trending

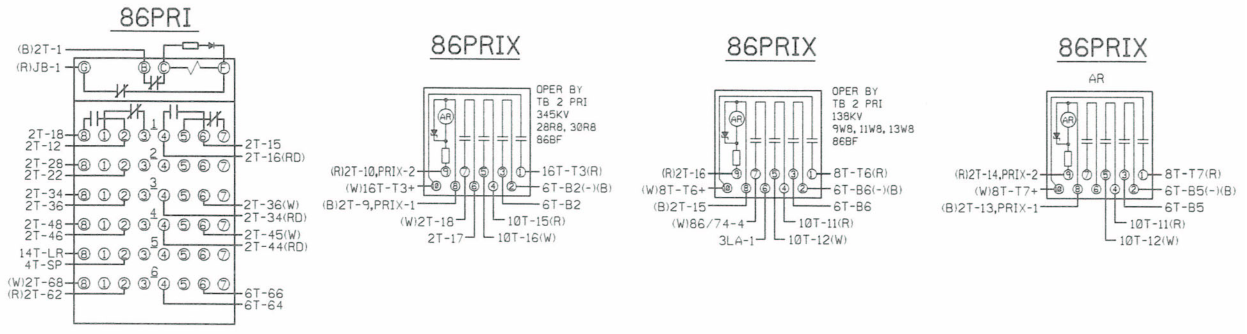


Figure 3 Wiring Required for Example Lockout Function

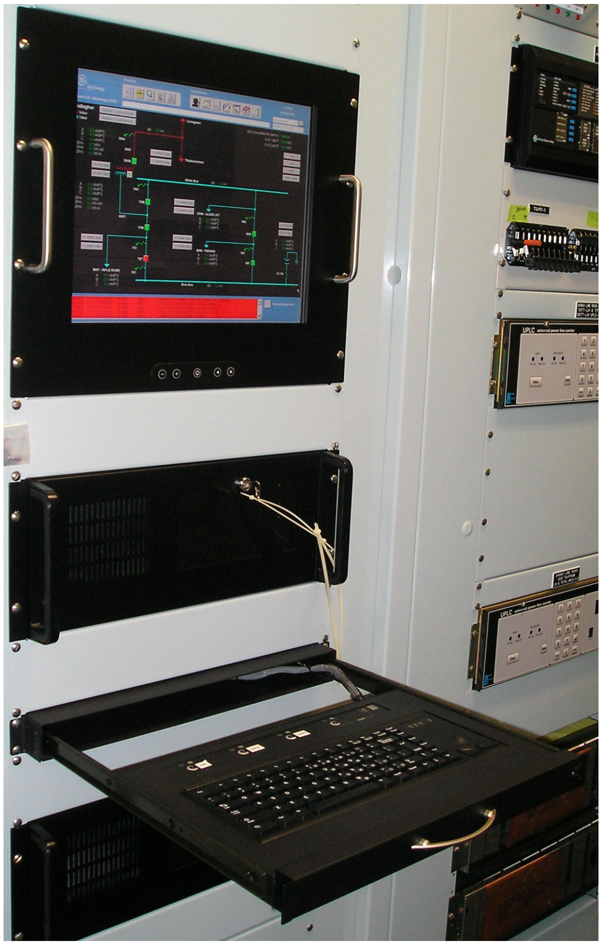


Figure 4 Substation Computer with HMI

time frames is captured by a DFR computer that gathers data from the redundant protective relays covering each zone (called dDFR host in Figure 1). The phasor measurement unit (PMU) function is also performed by the relays or by a networked PMU that communicates its phasor value packets on the LAN.

Handling these critical substation functions in such an unfamiliar new way naturally raises concerns among engineers, technicians, and maintenance personnel. It is not possible, nor necessarily desirable, to replicate the exact appearance and behavior of the conventional schemes. The recent creation of the METC organization, with little stake in the existing legacy designs, makes acceptance of such dramatic change easier.

Core Requirements and Critical Features of the Lockout Function

The functional requirements for most of the 12 functional items listed above are obvious to most relay and control engineers. However, using GOOSE messaging to perform the lockout switch function is a radical change and the path to accomplishing the function is not so clear. The new implementation will not look at all like the familiar lockout switch knob that twists with a bang when energized and takes a strong arm to reset. The lockout function, referred to by ANSI® device number 86, is defined as an electrically operated, hand or electrically reset device which functions to shut down and hold an equipment out of service, or both, upon occurrence of abnormal conditions. The simple core functions contained in this definition are designed into the system. However, through common practice, critical features of the lockout function have been established. Below is a list of the critical functions required of existing lockout schemes that must be captured in any new design, even though the means of meeting these requirements is totally changed. In the following list, the term lockout refers to what happens in today's schemes when a multitrip lockout switch operates.

1. Unique Lockout Function - Each protective function that performs lockout has its own lockout state, not combined with others. For example, if a transformer differential relay trips, it sets a lockout state for the breakers that isolate that transformer. If subsequent to the tripping operation, one of the breakers fails, then that breaker failure function sets a separate lockout state for the failed breaker and all the other breakers or TT channels used to isolate it. The failed breaker then has *two independent lockouts* applied to it.
2. Local Indication - An operator must be able to determine which of these individual lockouts are in effect, so he or she can check on the cause and remedy for each, and sign off on corrections before resetting each one.
3. Close Inhibit - A breaker cannot be closed as long as *any* lockout is still in effect, even if some lockouts applied to it have been reset.
4. Immunity to Relay Loss of Power - The application of the lockout must not be dependent on the life of any particular relay, or on power to the relay. In other words, failure of the controlling relay or its dc supply cannot possibly enable closing of a locked out breaker.
5. Immunity to System Loss of Power - The memory of each of the possible lockouts must be nonvolatile. In other words, even if the entire P&C system is deenergized and later reenergized, all the lockouts that were in effect must be remembered.

In addition to the critical features there are desired features that are intended to be included in the final design. The desired features include:

1. Remote Indication - The lockout states are reported to SCADA and to maintenance via the LAN and remote communications.
2. Single Procedure Reset - The resetting of a particular lockout has a single procedure - all the affected breakers, channels, and other systems are reset as a group *with respect to this particular lockout* when that resetting procedure is applied. The operator cannot be expected to routinely go around the station finding and resetting the lockout actions at each of many target relays, breakers, or channels.
3. Backup Indication and Reset - There must be a clear (not necessarily convenient) backup process for identifying and clearing lockouts per above rules if the substation concentrator, computer, or HMI are down.
4. Lockout Restored by System - Lockout memory must be robust in the face of relay failures and replacements. The system should have the means to align the picture of lockouts among all the relays and IEDs in the substation. If any is replaced, the system should be able to set its lockout states correctly when it is turned on, even though the replaced device was not there when the problem initially arose.

Beyond these, the new LAN-based implementation gives opportunities for new features. For example, the system can track when the lockout was applied, and which person removed it, including notes that person can enter when removing it. Removal of lockouts can be remotely blocked or overseen to prevent careless resetting by field personnel in a hurry. Back office applications can compile statistics on frequency, causes, time duration, and handling of lockout incidents for business process reporting and improvement.

Logic Design

Traditional Lockout Methods

Traditionally, protection and control lockout schemes consisted of single function protection relays, distance relays for example, which would operate a hard-wired lockout relay that would perform the tripping of the breakers and blocking of the closing on this same breaker. Sometimes, in transmission line applications where reclosing is a requirement on transient faults, the lockout function is used by backup protection functions like timed distance and breaker failure through direct transfer tripping. In transformer protection applications, it is used by all protection functions. Redundancy is a key aspect of all HV and EHV applications, and typically each scheme would have a lockout relay, meaning lots of wiring and panel space requirements.

Figure 5 shows part of a traditional implementation of a typical 345kV direct transfer tripping and close blocking lockout function. In Figure 5 the lockout function labeled **86TT** is being initiated from the transfer trip receive contact labeled **T**. In Figure 6, the **86TT** lockout relay Normally Open (NO) contact is wired to a generic lockout relay labeled **LOX**. The generic lockout relay **LOX** Normally Closed (NC) contact is wired to the closing interposing relay **P 52/X-1**, and a (NO) contact from **P 52/X-1** is wired in series with all close coils. If **86TT** is picked up, **LOX** is thus picked up, and the interposing close **P 52/X-1** can't close the breaker, thus is close blocking achieved from the lockout **86TT**. In Figure 7 another **86TT** lockout relay NO contact is wired directly to the trip circuit, in parallel with numerous other interposing and lockout relay contacts. This example illustrates an implementation that used numerous auxiliary devices since the amount of contacts on each device is limited. The consequence was that the required amount of wiring and complexity of the scheme were both increased.

New Distributed Lockout Methods

As technology has developed, more and more functions have been added to multi-functional protective relays, including the lockout function. However, distributed lockout functions were still not possible without any wiring between devices.

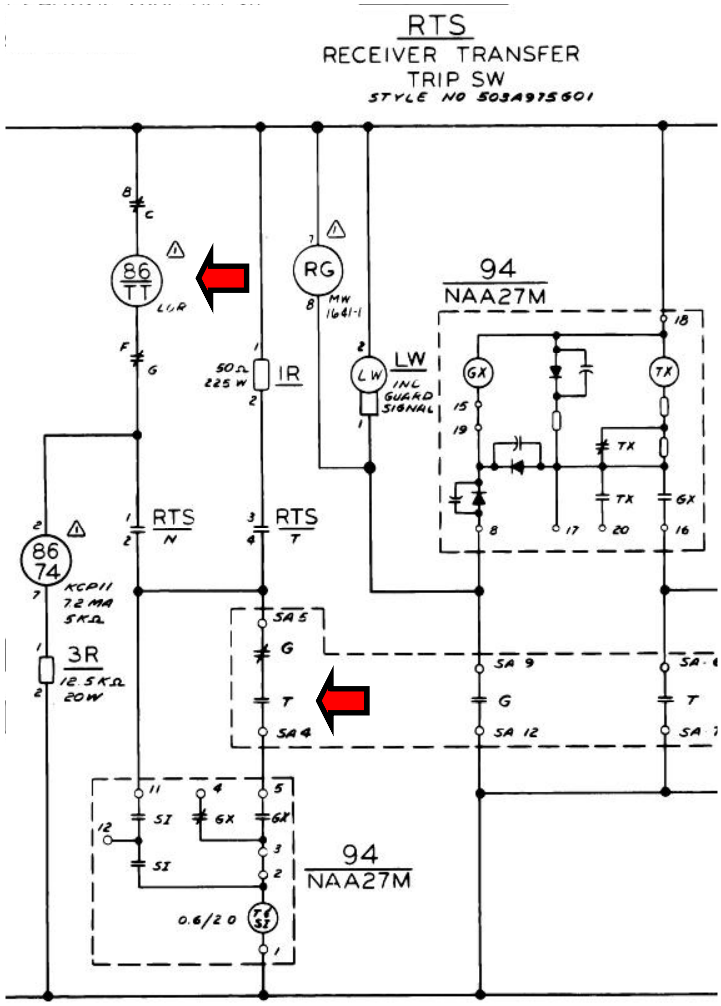


Figure 5 Initiation of a Lockout Function

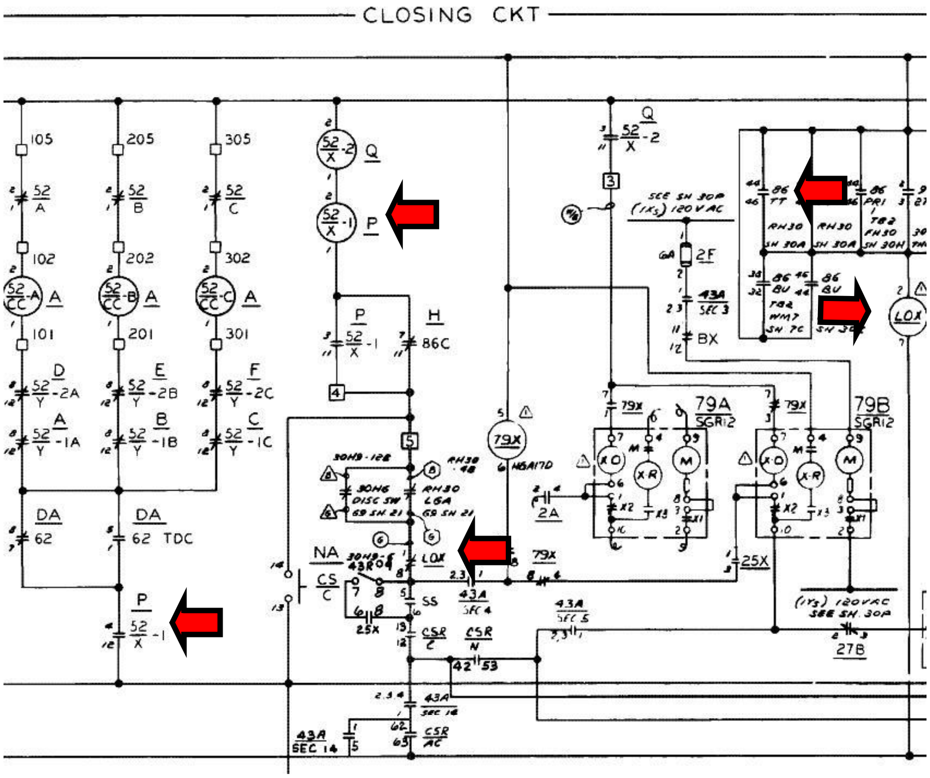


Figure 6 Close Inhibit Feature of Lockout Function

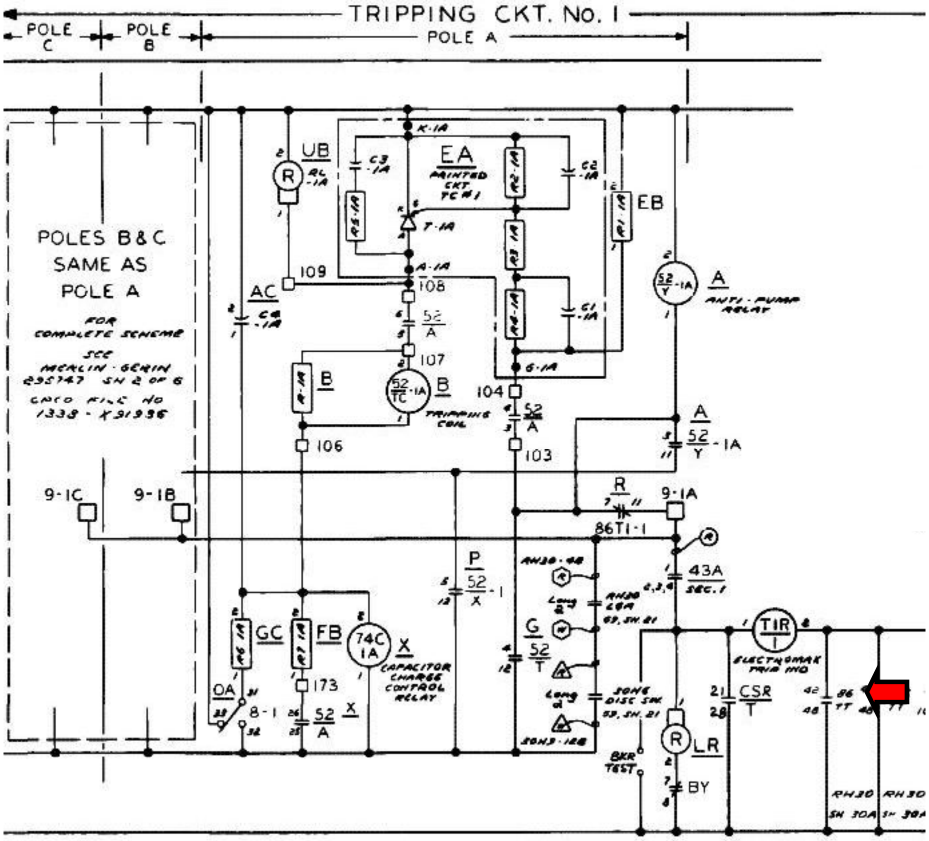


Figure 7 Tripping Action of Lockout Function

It is only when peer-to-peer inter relay communications came on the scene that distributed lockout functions became feasible. Unfortunately, protection relay vendors had their own initial implementation, until the IEC 61850 standard was issued. IEC 61850 allows multi-vendor applications where different vendor devices can be used to exchange digital Information consisting of statuses and commands for example [1].

With the ability to exchange data between IED's it became possible to start to implement multi-IED applications like special protection remedial action schemes and distributed lockout schemes. The latter will be described in more detail. Distributed lockout functions are essential in breaker fail applications, and any application where lockout over a larger distance or over the span of multiple IED's is desired. In these applications, it is essential that the lockout state be retained after the loss and regain of power. However, this has operational consequences if this is to happen, and will be discussed later. All the traditional inter-relay wiring can be replaced by inter-relay communications, utilizing the IEC 61850 standard, ensuring a scheme that can easily be expanded upon or revised.

The scheme must have the same reliability, or better, than the existing scheme. This can be achieved by utilizing two identical lockout schemes running in parallel, and each scheme has redundant communication channels with secure networks.

Philosophy of Distributed Lockout

A typical redundant lockout scheme, including transformer, 345kV and 138kV breaker failure protection can be implemented as shown in Figure 8. This scheme is based on protection schemes protecting one 345/138 kV transformer, one terminal of a 345kV line and one terminal of a 138kV line, thus a small station with two lines and one transformer. In this implementation the transformer relays are directly connected to the 138kV circuit breaker trip and close coils and the 345kV line relays are directly connected to the 345kV circuit breaker trip and close coils. This can easily be expanded upon if multiple circuits are present, but for simplicity only the above will be covered. For complete redundancy, two schemes per device are required, therefore there are six IEDs performing overall scheme protection. All latching functions described should be of the non-volatile type ensuring the state of the latch will be maintained during the loss of power. The main focus here is the logic configuration in the two 345kV line IEDs, though it should be very similar in the 138kV line IEDs. The operate and reset aspects of the lockout functions will be described separately.

The first part of the lockout scheme is the transformer protection operation that has to latch trip and lock out all close commands to both the 345kV and 138kV breakers. The transformer protection operation of system 1 set the latch within the transformer IED i.e. within itself, a latch within both systems 1 and 2 345kV line protection relays and both systems 1 and 2 138kV line protection relays. The latter part is not shown in the diagram. The set command from transformer 1 IED can be transported by means of GSSE messaging to the line IEDs. Each of these latches then ensures tripping and blocks closing of the local breaker. Each latch set is unique to the originating lockout function, this accomplishes the first critical feature. And all applicable latches must be reset before the close inhibit is removed. This addresses the third critical feature. Transformer differential operation of system 2 IED will result in the same latches being set, except for system 1 transformer IED.

The breaker failure trip function of the 138kV breaker that is located in 138kV line IED system 1, set the latches in both systems 1 and 2 345kV line IEDs. Breaker failure trip of 138kV system 2 line IED will result in the same latches being set, except for system 1 138kV line IED.

Breaker failure of the 345kV breaker of systems 1 and 2 345kV line IEDs should set only a latch in itself respectively, and key this information to the remote end of the 345kV line to ensure the line gets cleared.

Resetting of this logic becomes a challenge, and great care should be taken to ensure that when a function is reset in an IED, that it would reset all latches that was set, for example, if transformer IED system 1 operated, the local resetting of this function should reset all local and remote latches. This scheme provides the first desired feature. The same principle should apply for the breaker failure

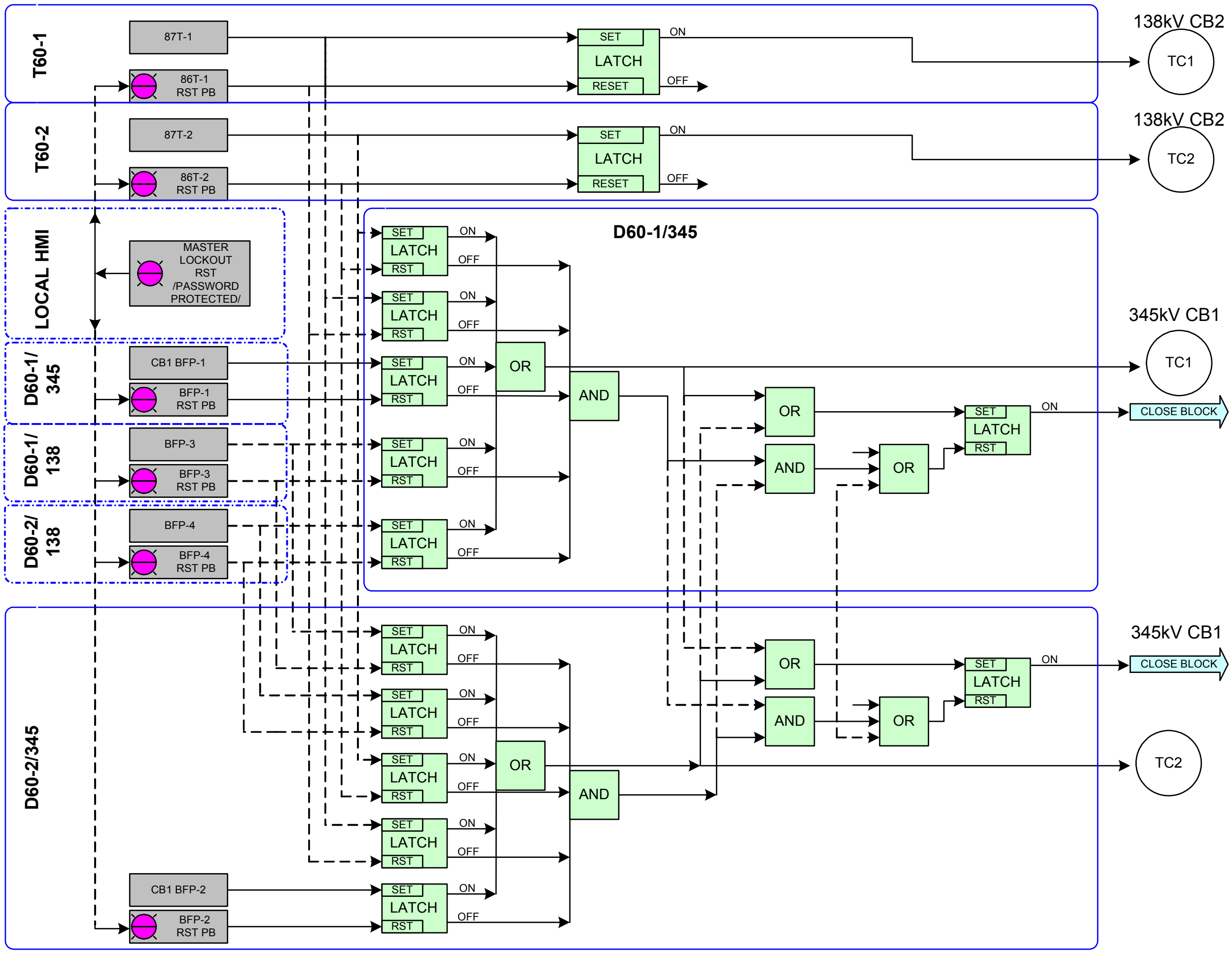


Figure 8 Logic Diagram for Distributed Lockout

functions. Since there is a risk that some of the devices can be offline (due to loss of power or communications), a master reset feature has to be available that these devices can be reset remotely, as is indicated by the HMI master lockout reset.

The lockout scheme described includes the following advantages and disadvantages:

Advantages

- Compared to traditional lockout schemes, the scheme is less complex, since no auxiliary equipment (except for the communications equipment) is required.
- Multiple repetitions can be performed expanding the overall lockout scheme without the need to add any additional hardware or wiring (if all IEDs are connected to the same communications infrastructure).

Disadvantages

- The scheme is heavily dependant on inter-IED communications, which becomes a key aspect of the required hardware.
- Setting and resetting of the lockout scheme becomes an issue if some devices are off-line

To address the disadvantages the following should be considered during implementation:

- All lockout latch functions should be of the non-volatile type, and maintain their state after power was cycled to the IED.
- Communications to each device should preferably be redundant, reducing the risk of loss of communications
- The output contacts associated with each lockout within each IED should preferably be of the lockout type, and thus should not change state if the IED was to loose power
- The lockout functions of systems 1 and 2 should preferably be separated from each other to minimize inter-system communications, and to allow one system, or parts of it, to be taken out of service for maintenance and testing.

Relay Configuration

Implementation Using IEC 61850

During implementation of lockout functions within multiple IEDs it is thus paramount that all IEDs have the inter-IED communications capabilities, more specifically, each device would need to be able to communicate to each other required IED using the GSSE messaging for transport of digital information, as is specified by the IEC 61850 standard. It is important to use this standard to ensure future expansion of the system, and that multi-vendor devices can be utilized in building the lockout functions.

Figure 9 is a detail of the communications architecture that supplies the redundancy expected to maintain the reliability for this LAN based solution. In this architecture, there are two redundant systems, System 1 and System 2. In addition, each IED in each system has redundant connections to the LAN. If one connection fails, the IED switches over to the other connection to maintain communication with the LAN.

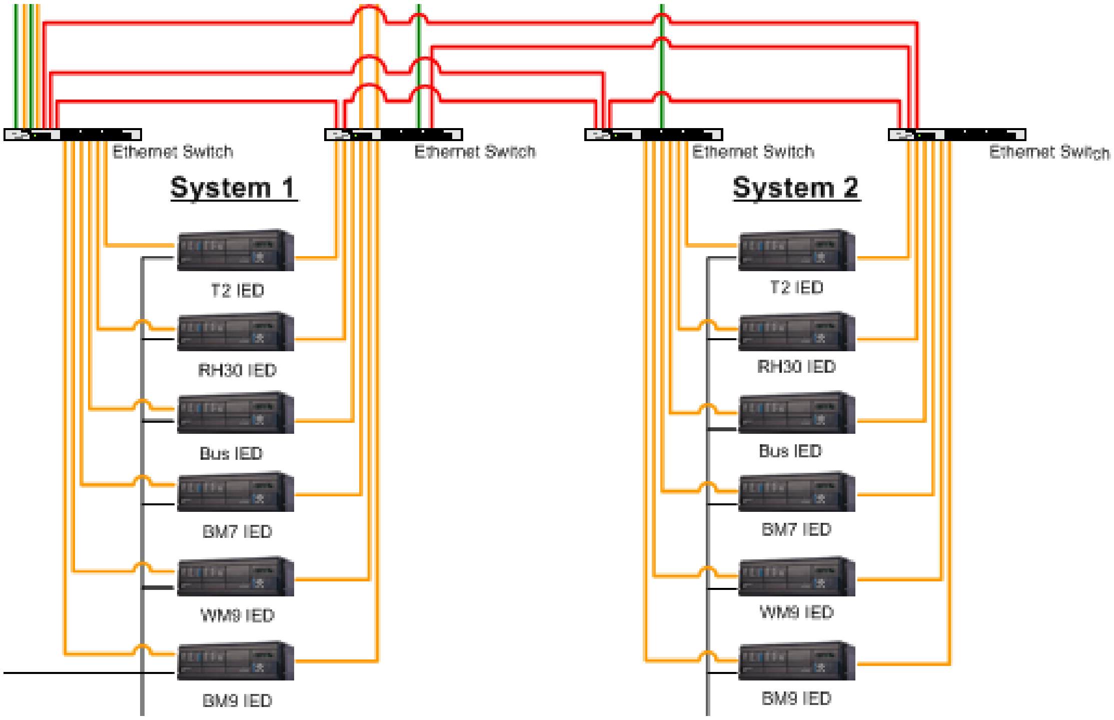


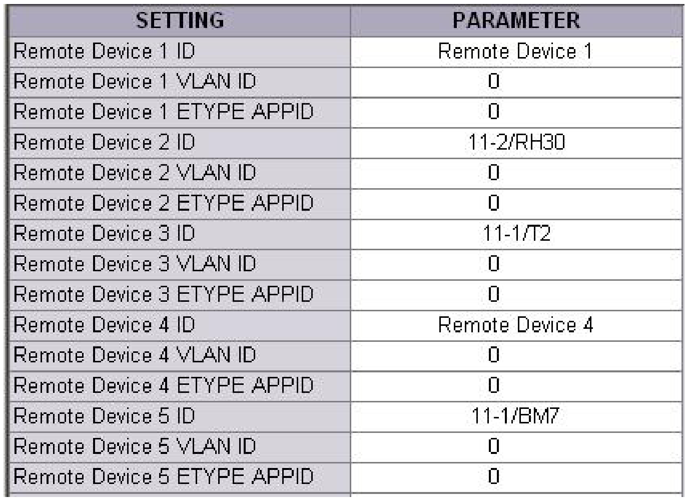
Figure 9 Detail of LAN Architecture

<u>Sample Implementation</u>

In implementing the above-mentioned requirements, a couple of steps have to be followed to ensure successful communications and lockout logic implementations:

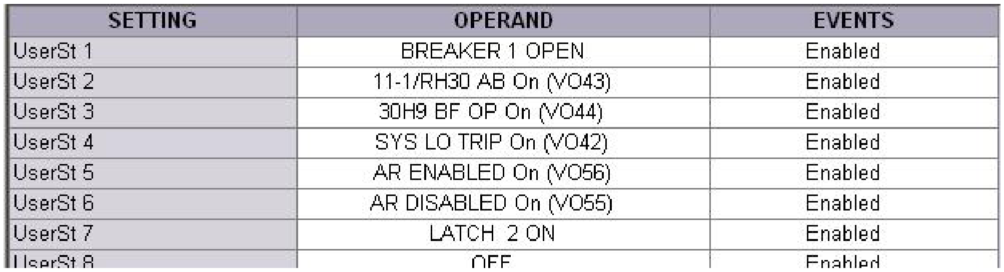
- Device Definition
  Each IED has to be assigned a recognizable name by which it will be known to other IEDs on the network. For our example, the assigned names are:
    - System 1 Transformer Protection IED: 11-1/T2
    - System 2 Transformer Protection IED: 11-2/T2
    - System 1 345kV Line Protection IED: 11-1/RH30
    - System 2 345kV Line Protection IED: 11-2/RH30
    - System 1 138kV Line Protection IED: 11-1/BM7
    - System 2 138kV Line Protection IED: 11-2/BM7

- Remote Device Definition
  Each IED has to be assigned a list of devices from which it will be expecting messages. Here is an example of how system 1 345kV Line Protection IED 11-1/RH30 was configured: (Note that only the devices on the network that need to be accessed are configured; not all devices)



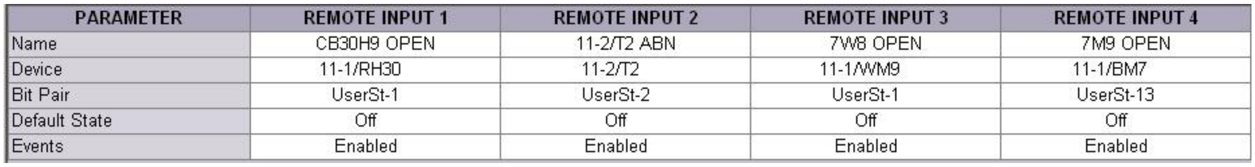
SETTING	PARAMETER
Remote Device 1 ID	Remote Device 1
Remote Device 1 VLAN ID	0
Remote Device 1 ETYPE APPID	0
Remote Device 2 ID	11-2/RH30
Remote Device 2 VLAN ID	0
Remote Device 2 ETYPE APPID	0
Remote Device 3 ID	11-1/T2
Remote Device 3 VLAN ID	0
Remote Device 3 ETYPE APPID	0
Remote Device 4 ID	Remote Device 4
Remote Device 4 VLAN ID	0
Remote Device 4 ETYPE APPID	0
Remote Device 5 ID	11-1/BM7
Remote Device 5 VLAN ID	0
Remote Device 5 ETYPE APPID	0

- Remote Outputs going to any external IED
  The Outputs that are allowed to go to any external IED has to be assigned. Here is an example of how remote outputs were configured in system 1 345kV Line Protection IED 11-1/RH30:



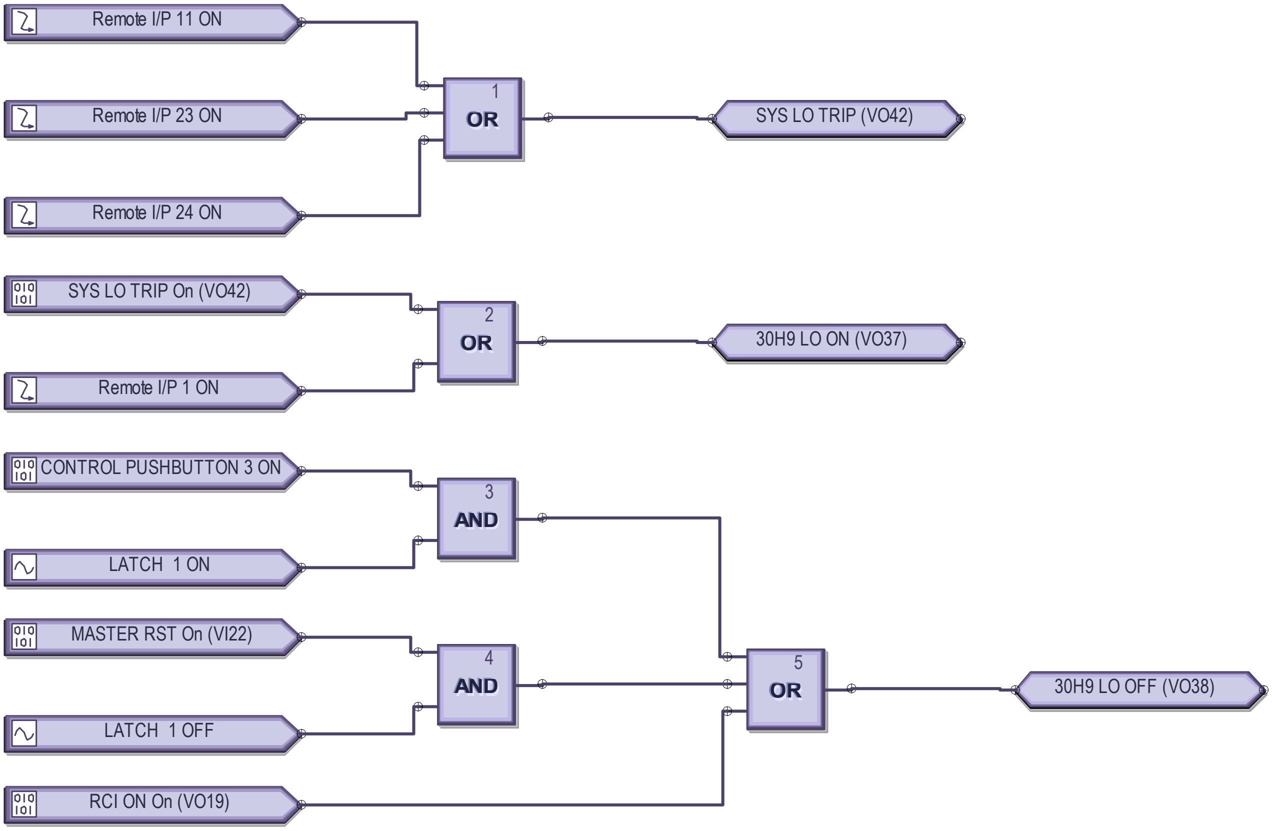
SETTING	OPERAND	EVENTS
UserSt 1	BREAKER 1 OPEN	Enabled
UserSt 2	11-1/RH30 AB On (VO43)	Enabled
UserSt 3	30H9 BF OP On (VO44)	Enabled
UserSt 4	SYS LO TRIP On (VO42)	Enabled
UserSt 5	AR ENABLED On (VO56)	Enabled
UserSt 6	AR DISABLED On (VO55)	Enabled
UserSt 7	LATCH 2 ON	Enabled
UserSt 8	OFF	Enabled

- Remote Inputs coming from external IEDs
  The remote signals coming from remote IEDs need to be defined, indicating for each signal from which IED and what remote output will be used for each particular defined input. Here is an example of how system 1 Transformer Protection IED 11-1/T2 was configured: (Most IED vendors developing IEC 61850 devices are starting to use a graphical representation of remote outputs and inputs)



PARAMETER	REMOTE INPUT 1	REMOTE INPUT 2	REMOTE INPUT 3	REMOTE INPUT 4
Name	CB30H9 OPEN	11-2/T2 ABN	7W8 OPEN	7M9 OPEN
Device	11-1/RH30	11-2/T2	11-1/WM9	11-1/BM7
Bit Pair	UserSt-1	UserSt-2	UserSt-1	UserSt-13
Default State	Off	Off	Off	Off
Events	Enabled	Enabled	Enabled	Enabled

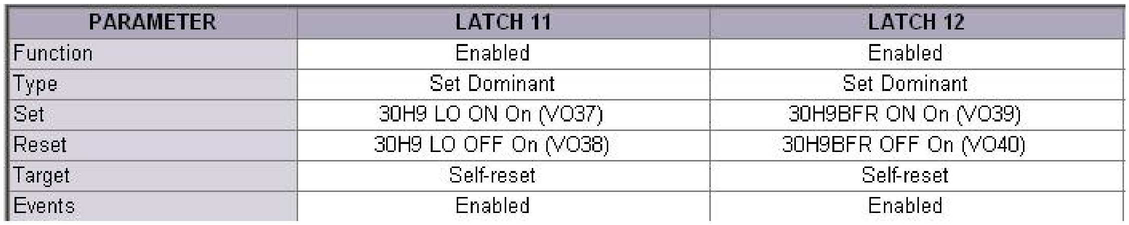
- Lockout Logic Development
  The lockout functions then have to be implemented in each IED, utilizing all used Remote inputs and local functions. Here is an example of how the close inhibit was implemented in system 1 345kV Line Protection IED 11-1/RH30 (Note that VO37 30H9 LO ON goes to the SET function of the non-volatile latch 11, and VO38 30H9 LO OFF goes to the RESET function of latch 11):



In the lockout logic, Remote Input 11 is assigned as the transformer protection trip from system 1 transformer protection IED 11-1/T2, which first goes to VO42 SYS LO TRIP. VO42 then goes to VO37 30H9 LO ON.

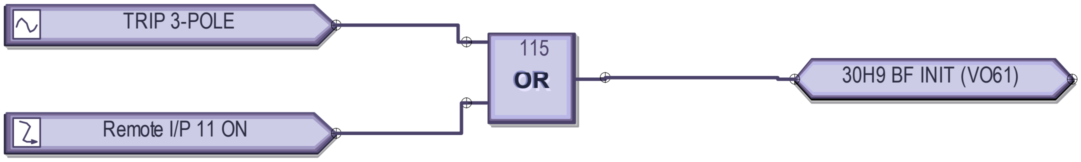
To satisfy the reset features needed for the lockout function, the lockout can be reset from a local push button and from the remote HMI. In Figure 8 the reset can be seen as originating from the Local HMI or, when under a contingency situation, such as the LAN being down, the reset can be performed at the IED using the assigned push button.

Non-Volatile Latches 11 and 12 were assigned as follows:

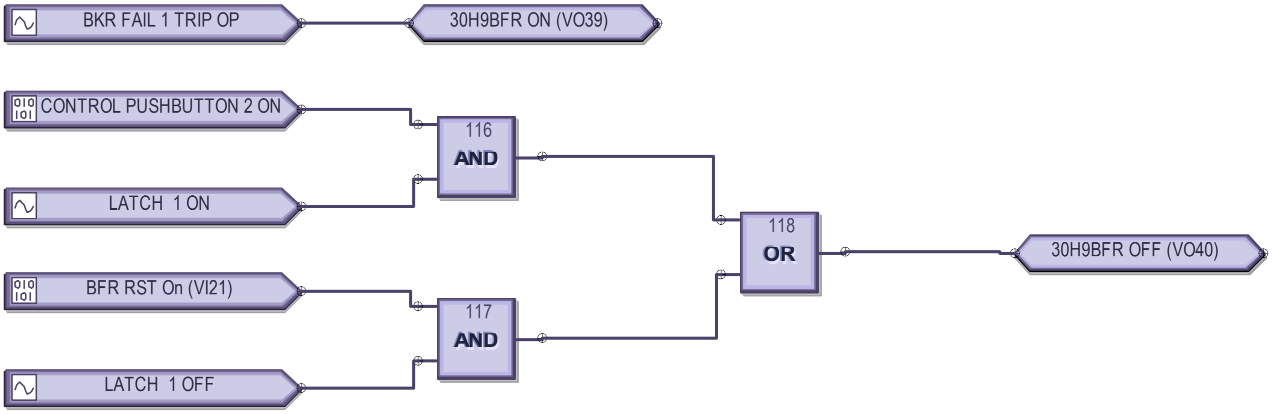


PARAMETER	LATCH 11	LATCH 12
Function	Enabled	Enabled
Type	Set Dominant	Set Dominant
Set	30H9 LO ON On (VO37)	30H9BFR ON On (VO39)
Reset	30H9 LO OFF On (VO38)	30H9BFR OFF On (VO40)
Target	Self-reset	Self-reset
Events	Enabled	Enabled

Latch 11 was used above to implement the close inhibit in system 1 345kV Line Protection IED 11-1/RH30. Latch 12 is used for the breaker failure lockout of the circuit breaker designated as 30H9. This example of the lockout function is implemented in system 1 345kV Line Protection IED 11-1/RH30. The initiate signal to the local breaker fail, consists of any local trip, or the transformer lockout trip as follows:



The SET and RESET functions of non-volatile latch 12 was created as follows:



Similar to the transformer lockout described previously, the breaker fail lockout can also be reset from a local push button or the HMI.

Implementing and Testing the Distributed Lockout Function

Implementing the distributed lockout in the control house addressed the final features of the lockout function. Local indication of the lockout function refers to the indication on the IED that is sending the lockout and the IED that is receiving the lockout. The lockout status is communicated at the IED through the use of LEDs on the front of the IED. Figure 10 shows the front of the IED. The LEDs are in the center of the IED. The pushbuttons under the LEDs will be used in the lockout function for resetting the lockout function if the LAN is down.

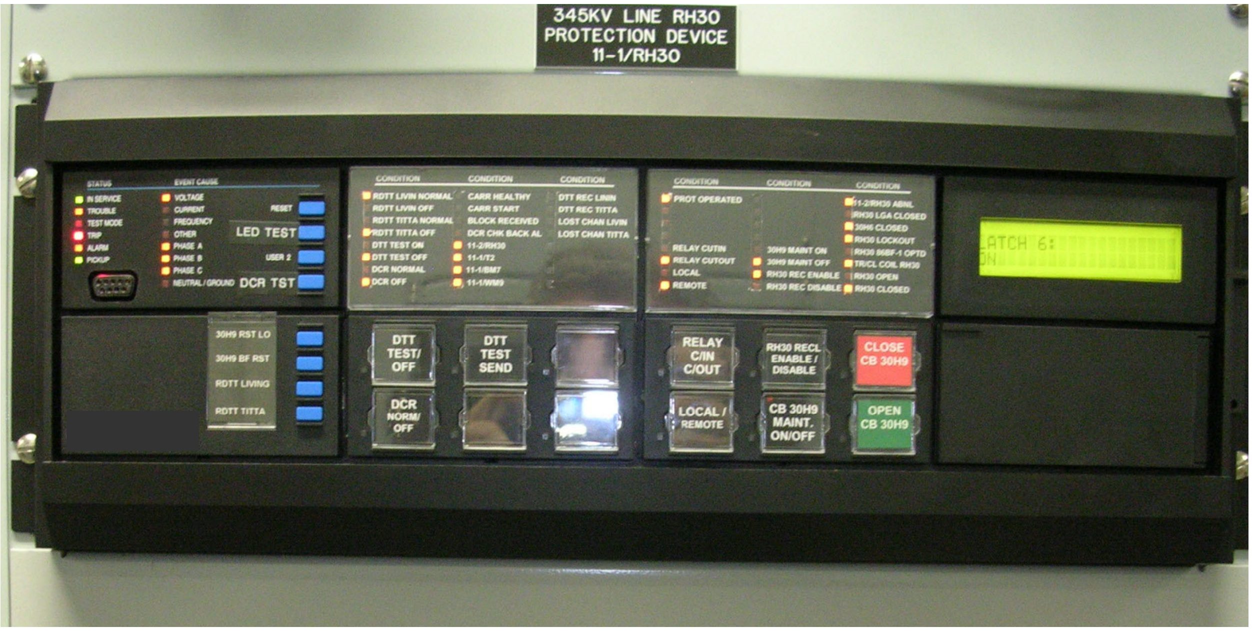
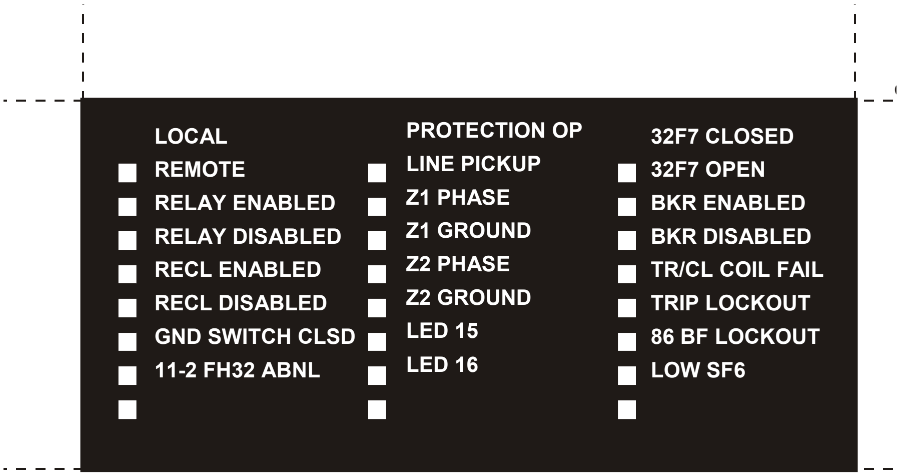


Figure 10 Front View of 11-1/RH30 IED

Figure 11 is a detail of the LED arrangement. In Figure 11, TRIP LOCKOUT refers to a lockout function in effect on the IED and 86 BF LOCKOUT refers to the breaker failure lockout function that is controlled by this IED. The IED allows great flexibility in assigning and labeling the LEDs.

Remote indication refers to indication remote to the IED. This includes both the indication at the HMI and offsite. This paper will cover the indication at the local HMI. Figure 12 shows the HMI after the breaker failure of circuit breaker 9B7. Since 9B7 has failed it is still closed (red) while the two adjacent breakers, 7B7 and 9M9, are open (green). In addition, the adjacent breakers indicate the locked out status by flashing a white X in the breaker symbol.

The reset action of the lockout function is designed to usually be performed at the HMI. The lockout screen, Figure 13, lists all possible lockout actions and resets for each. During a lockout, the green RESET is replaced with a red LOCKOUT. Note in Figure 13 that there is a also master lockout reset that allows resetting all lockout functions with one action.



	LOCAL		PROTECTION OP		32F7 CLOSED
□	REMOTE	□	LINE PICKUP	□	32F7 OPEN
□	RELAY ENABLED	□	Z1 PHASE	□	BKR ENABLED
□	RELAY DISABLED	□	Z1 GROUND	□	BKR DISABLED
□	RECL ENABLED	□	Z2 PHASE	□	TR/CL COIL FAIL
□	RECL DISABLED	□	Z2 GROUND	□	TRIP LOCKOUT
□	GND SWITCH CLSD	□	LED 15	□	86 BF LOCKOUT
□	11-2 FH32 ABNL	□	LED 16	□	LOW SF6
□		□		□	

Figure 11 Detail of IED LED Arrangement

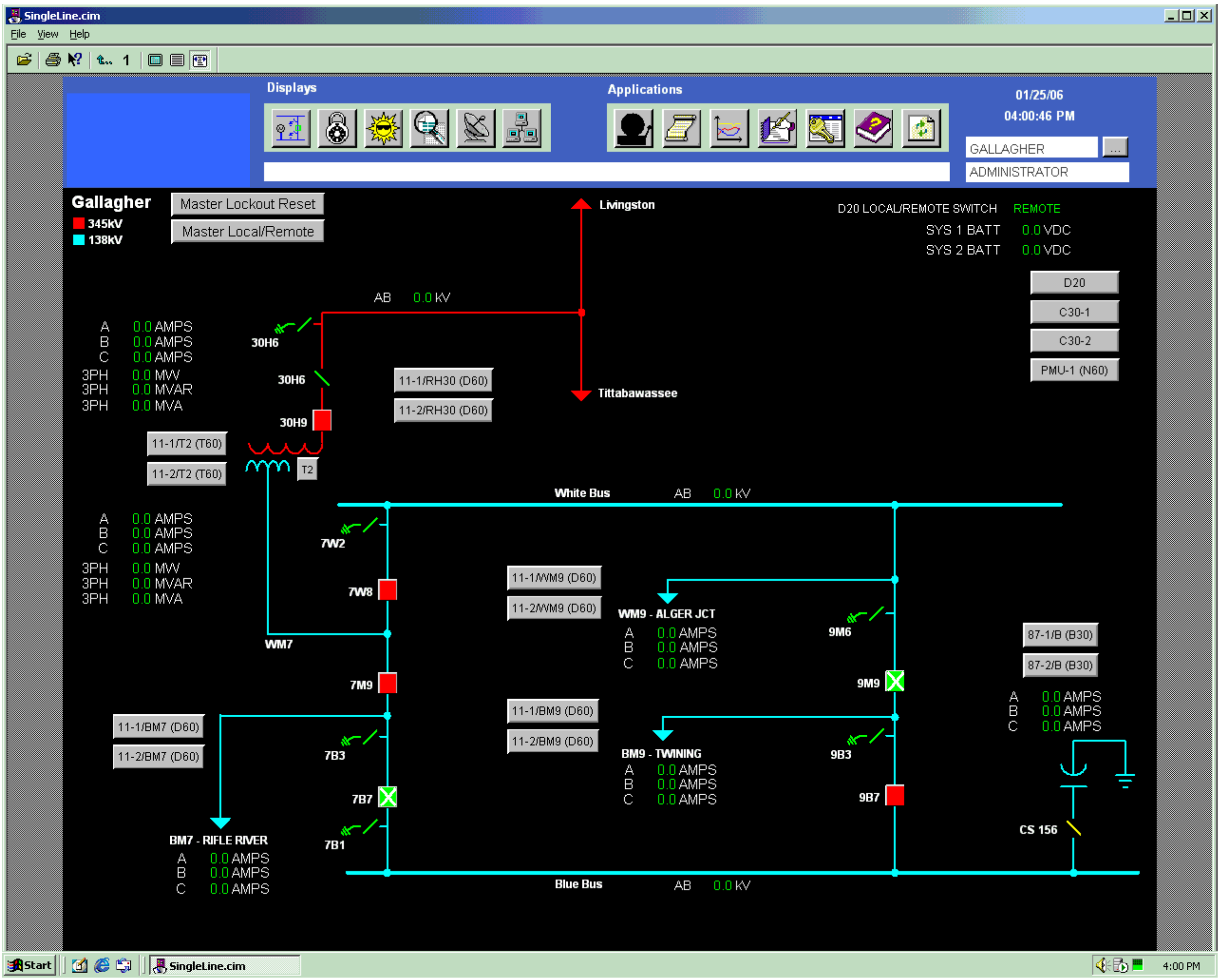
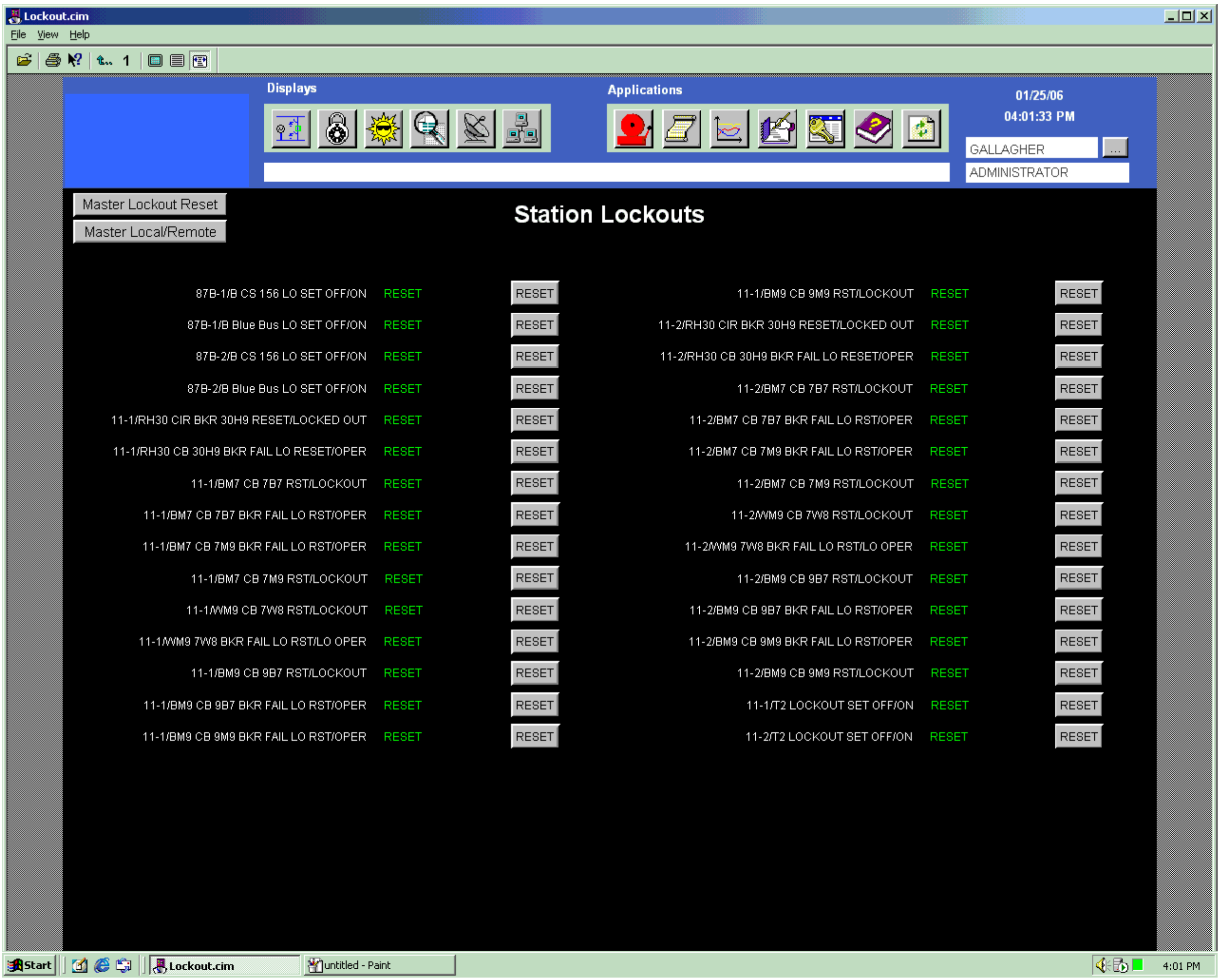


Figure 12 HMI Displaying Breaker Failure of 9B7

Testing the lockout function occurs during two phases of the control house. The two phases of testing are the factory acceptance test (FAT) and the site acceptance test (SAT). The FAT was performed off site where the system was assembled. Most of the features of the lockout function are simple in nature however there are a few aspects of the FAT that deserve attention.

As has been detailed, the wiring of the substation has been for the most part replaced with the logic configuration inside each IED. Wiring is tested by lamping wires and yellowing wiring diagrams. A process for assuring the quality of the relay configuration was needed to maintain the same level of thoroughness. The logic configuration of each IED was collected on a series of logic diagrams that graphically represent the programming of the IEDs. With this in hand, each logic point is verified by monitoring the IEDs and yellowing out the logic diagram as each part of the configuration is confirmed.

Next, the operating time of the distributed lockout is considered due to the operating differences between it and the EM implementation of the lockout function. The time it takes to initiate and operate the EM lockout is a function of the mechanical design of the lockout. Note that the time it takes for the initiating protection to get its “message” to the EM is instantaneous however there is time necessary for the lockout relay to unlatch, rotate, and close its contacts. The operation time of the lockout relay is approximately one cycle or 16ms.



01/25/06
04:01:33 PM
GALLAGHER
ADMINISTRATOR

Station Lockouts

87B-1/B CS 156 LO SET OFF/ON	RESET	RESET	11-1/BM9 CB 9M9 RST/LOCKOUT	RESET	RESET
87B-1/B Blue Bus LO SET OFF/ON	RESET	RESET	11-2/RH30 CIR BKR 30H9 RESET/LOCKED OUT	RESET	RESET
87B-2/B CS 156 LO SET OFF/ON	RESET	RESET	11-2/RH30 CB 30H9 BKR FAIL LO RESET/OPER	RESET	RESET
87B-2/B Blue Bus LO SET OFF/ON	RESET	RESET	11-2/BM7 CB 7B7 RST/LOCKOUT	RESET	RESET
11-1/RH30 CIR BKR 30H9 RESET/LOCKED OUT	RESET	RESET	11-2/BM7 CB 7B7 BKR FAIL LO RST/OPER	RESET	RESET
11-1/RH30 CB 30H9 BKR FAIL LO RESET/OPER	RESET	RESET	11-2/BM7 CB 7M9 BKR FAIL LO RST/OPER	RESET	RESET
11-1/BM7 CB 7B7 RST/LOCKOUT	RESET	RESET	11-2/BM7 CB 7M9 RST/LOCKOUT	RESET	RESET
11-1/BM7 CB 7B7 BKR FAIL LO RST/OPER	RESET	RESET	11-2/WM9 CB 7W8 RST/LOCKOUT	RESET	RESET
11-1/BM7 CB 7M9 BKR FAIL LO RST/OPER	RESET	RESET	11-2/WM9 7W8 BKR FAIL LO RST/LO OPER	RESET	RESET
11-1/BM7 CB 7M9 RST/LOCKOUT	RESET	RESET	11-2/BM9 CB 9B7 RST/LOCKOUT	RESET	RESET
11-1/WM9 CB 7W8 RST/LOCKOUT	RESET	RESET	11-2/BM9 CB 9B7 BKR FAIL LO RST/OPER	RESET	RESET
11-1/WM9 7W8 BKR FAIL LO RST/LO OPER	RESET	RESET	11-2/BM9 CB 9M9 BKR FAIL LO RST/OPER	RESET	RESET
11-1/BM9 CB 9B7 RST/LOCKOUT	RESET	RESET	11-2/BM9 CB 9M9 RST/LOCKOUT	RESET	RESET
11-1/BM9 CB 9B7 BKR FAIL LO RST/OPER	RESET	RESET	11-1/T2 LOCKOUT SET OFF/ON	RESET	RESET
11-1/BM9 CB 9M9 BKR FAIL LO RST/OPER	RESET	RESET	11-2/T2 LOCKOUT SET OFF/ON	RESET	RESET

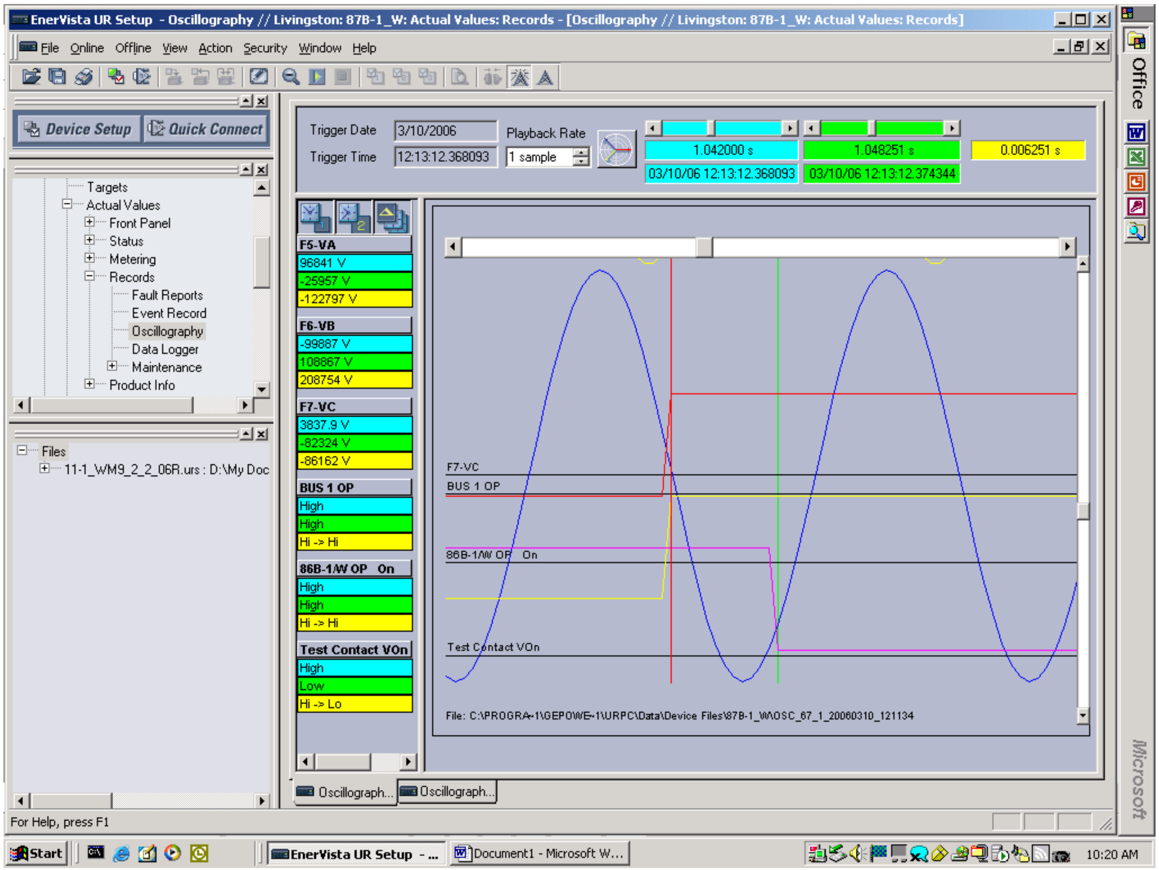
Figure 13 HMI Lockout Screen

For the distributed lockout there is propagation time for the message to get from the publishing IED to the subscribing IED. This propagation time is designed to be a fraction of a cycle. The operating time of the distributed lockout function was demonstrated during the FAT.

Another protection function that will be using GOOSE messages and the lockout function is protection of the 138kV bus. 86B-1/W is an IED that will be used to protect the bus. It will be sending a message to the 11-1/WM9 IED that trips the breaker and locks it out. The initiation of the virtual output that sends the message is compared to the closing of the output contacts that trip the breaker.

Figure 14 shows the oscillography from this demonstration. The initiation of the message is indicated by the trace labeled 86B-1/W OP On. This is the digital trace that is just below the 86B-1/W OP On label. It starts low and goes high and is equivalent to the trace labeled BUS 1 OP. This trace reaches the high state at the time of 1.042s. The closing of the output contact is tracked by the trace labeled Test Contact Von. It is the digital signal that starts high and goes low. This trace reaches the low state at the time of 1.048251s. The difference is 6.251ms. This compares favorably with the operating time of the EM lockout relay, which is estimated at 1 cycle or 16.7ms.

There is one aspect of the distributed lockout that is not addressed by the demonstration above. The propagation time of the GOOSE message can be effected by the amount of traffic on the LAN. As data queues up to pass through the Ethernet switches the data could get held up. Qualitatively, this time delay



Trigger Date 3/10/2006
Trigger Time 12:13:12.368093
Playback Rate 1 sample

1.042000 s | 1.048251 s | 0.006251 s
03/10/06 12:13:12.368093 | 03/10/06 12:13:12.374344

F5-VA		
96841 V	-25957 V	-122797 V
F6-VB		
-99887 V	108867 V	208754 V
F7-VC		
3837.9 V	-82324 V	-86162 V
BUS 1 OP		
High	High	Hi -> Hi
86B-1/W OP On		
High	High	Hi -> Hi
Test Contact VOn		
High	Low	Hi -> Lo

File: C:\PROGRA~1\GEPOWE~1\URPC\Data\Device Files\87B-1_W\OSC_67_1_20060310_121134

Figure 14 Oscillography of Distributed Lockout Timing Test

should be negligible due to the expected level of LAN traffic. There are steps that can be taken to make this time even shorter. IEC 61850 has the option of assigning a priority level to the message that allows designated messages to skip to the front of the line.

The SAT will include a quantitative review of how expected traffic will affect the delivery of GOOSE messages. It will also include the assessment of this delivery during a hypothetical data storm. At the time of this writing the SAT is still in the planning stage.

Conclusions

It has been shown that IEC 61850 has enabled the implementation of the lockout function in a distributed method. The manner of this implementation has been shown including how the function has been designed, configured and tested. Along the way the benefits of this implementation have been illustrated along with operating issues and further tests that need to be addressed.

The most important conclusion to draw is how this implementation is consistent with the technical strategy of METC. It greatly reduces the quantity of equipment, wiring, and space since the lockout device and its associated wiring is no longer needed. It obviously reduces installation costs but in addition operating costs are reduced. Since the lockout function operates over the LAN, system reconfiguration (e.g. the addition of high voltage circuit breakers) that would require rewiring in the past is addressed through changes in the logic. The system also allows for rapid status reports on the lockout function. If any portion of the network is compromised, thereby compromising the lockout function, immediate indication is made and action can be taken. All indications of the application of IEC 61850 to perform the lockout function are that it is a success. The final testing to take place soon will confirm this.

References

1. IEC 61850 Standard, *Communications Networks and Systems in Substations*, 10 parts dated from 2001 to 2005.
2. IEEE C37.115-2003, *IEEE Standard Test Method for Use in the Evaluation of Message Communications between Intelligent Electronic Devices in an Integrated Substation Protection, Control, and Data Acquisition System.*
3. IEEE 1613-2003, *IEEE Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations.*

Biographies

Robert Brantley is a Senior Control and Monitoring Systems Engineer at Michigan Electric Transmission, LLC. He is currently serving as the project manager for METC's Substation Automation and SCADA/Wide Area Telecommunications Initiatives. Mr. Brantley earned his bachelor's of science degree in electrical engineering technology from Georgia Southern University.

Kevin Donahoe P.E. has spent the last 25 years working in the electric utility industry. The last twenty two of those years have been spent testing, installing, trouble shooting, specifying, setting, estimating, designing, reviewing, documenting, and setting standards for protection and control schemes. Mr. Donahoe spent 20 years with Commonwealth Edison, an Exelon company, before moving to GE NRPS. Though the majority of Mr. Donahoe's experience has been with transmission and distribution substations he has significant experience with generation protection and distribution protection with specific experience with interconnection requirements. Before all that Mr. Donahoe received his BSEE from the Illinois Institute of Technology in 1981 and in 1993 received an MBA from Lewis University. Mr. Donahoe is a member of the IEEE Power System Relaying Committee and the IEEE Standards Advisory. He is a Licensed Professional Engineer in Illinois, Oklahoma, and Michigan.

JC (Jacobus) Theron received the degree of Electrical and Electronic Engineer from the University of Johannesburg, South Africa in 1991. Mr. Theron has 15 years of engineering experience including from 1992 to 1997 for Eskom (South Africa) as Protection, Control and Metering Engineer, from 1999 to 2002 for GE Multilin (Canada) as Protective Relaying Consultant, for 2002 and 2003 for Alstom T&D (USA) as Senior Systems Engineer and since 2003 for GE Multilin (Canada) as Protection and Systems Engineer, leading the Project and Consulting Engineering team. He specializes in transmission, distribution and rotating machines protection applications support, system designs and transient system testing.

Eric A. Udren has a 35 year distinguished career in design and application of protective relaying and control systems. He received his BSEE from Michigan State University in 1969, MSEE degree from New Jersey Institute of Technology in 1981, and the Certificate of Post-Graduate Study in Engineering from the University of Cambridge (UK) in 1978. He worked in protective relay design and application with Westinghouse and its successor ABB from 1969 to 1996. In 1969 he developed software for the world's first computer-based relaying system. From 1978 to 1986, he supervised relaying and control software development for the EPRI-sponsored first development of a LAN-based integrated protection and control system. In 1996, he joined Eaton Electrical (Cutler-Hammer), where he served as Engineering Manager for Metering and Protection Development. In 2004, Mr. Udren joined KEMA T&D Consulting. He maintains his office in Pittsburgh. Working with KEMA, Mr. Udren has developed the technical strategy for some of the most progressive utility LAN-based substation protection and control upgrading programs using IEC 61850 and other data communications. Mr. Udren is a Fellow of IEEE, Member of the IEEE Power System Relaying Committee (PSRC), and Chairman of two PSRC Standards Working Groups. In 2001, he received the PSRC Distinguished Service Award. In 2006 he received the PSRC Distinguished Service Award for Coordination of International Standards Activities. He serves as Technical Advisor to the US National Committee of the IEC for TC 95, Measuring Relays. He also serves as a US Delegate to IEC TC 57 Working Group 10 responsible for IEC 61850. He has written and presented over 40 technical papers and chapters of books on relaying topics.