Enhancing Power System Automation Through the Use of Real-Time Ethernet

Veselin Skendzic and Armando Guzmán
Schweitzer Engineering Laboratories, Inc.

Presented at the
5th Annual Clemson University Power Systems Conference
Clemson, South Carolina
March 14–17, 2006

Originally presented at the
DistribuTECH Conference, January 2005

ENHANCING POWER SYSTEM AUTOMATION THROUGH THE USE OF REAL-TIME ETHERNET

Veselin Skendzic and Armando Guzmán
Schweitzer Engineering Laboratories, Inc.
Pullman, WA USA

ABSTRACT

Since its inception in the early seventies, Ethernet technology has experienced wide acceptance and has exhibited exponential growth. It was only recently that Ethernet managed to virtually displace competing process bus and local area network (LAN) technologies—Token Ring, Profibus, Modbus® Plus, LonWorks®, etc.—most of which had to switch to the Ethernet-based physical layer and TCP/IP-based protocols (Modbus TCP/IP, Profibus TCP/IP, and DNP TCP/IP).

Ethernet is still widely believed to be inadequate for mission-critical, hard real-time applications because of inherent limitations associated with the traditional collision-based access techniques. However, fostered by the development of international standards (IEEE 802.3x, 802.1q, 802.1p, 802.1w, IEC 61850-x-x), Ethernet has now evolved into a highly predictable and reliable real-time network technology.

This paper provides an overview of the latest standards and investigates their impact on power system automation and protection. We give special attention to the use of the IEC GOOSE and IEC GSSE messages and to new options for streaming analog data over Ethernet described in IEC 61850-9-2.

The paper includes application examples describing use of real-time Ethernet in distribution substation and industrial plant automation, such as fast bus trip, permissive transfer trip, and network reconfiguration-based breaker failure protection.

INTRODUCTION

Digital communications have slowly become an indispensable part of the electric utility network. While not directly involved in the bulk power transfer, digital communication infrastructure is an essential ingredient without which large interconnected power systems cannot operate.

Recent events like the August 14th, 2003, blackout emphasized the need for improved data collection and real-time situational awareness. These events provide additional impetus for deployment of new technologies such as synchrophasors, application of GPS-based global time dissemination, substation Ethernet, and better use of existing microprocessor relay/Intelligent Electronic Device (IED) capabilities.

Improved digital communications are also causing legacy device consolidation [1], making it increasingly more difficult to distinguish the SCADA remote terminal unit (RTU) functionality from a communications processor, protective relay, revenue meter, bay controller, or a digital fault recorder.

Technology is evolving such that, in the near future, all of the above devices could merge into a single multifunction unit capable of performing any subset of power system automation and control functions. While such a "merger" may not be imminent, it is interesting to note important

integration trends being set by international standards, most notably IEC 61850. This standard intentionally separates application data, data transfer services, and communication protocols so that functions can be "merged" or distributed among any number of devices.

The IEC 61850 effort titled "Communication networks and systems in substations" comprises 12 published standards, with the 13th nearing completion [2] [3]. Although originally envisioned for use within the substation, IEC 61850 is currently being extended to encompass communications between substation and the control center, thus becoming a real SCADA protocol. In this role, IEC 61850 is expected to slowly replace IEC 60870-5-101, (-104) and DNP3. In addition to including SCADA functionality and emphasis on substation data object models and service definitions, IEC 61850 also includes four real-time mechanisms aimed at time-critical protective relay communications and sampled analog data streaming.

IEC 61850 has managed to span much of the application space, thus providing solid basis for building reliable and interoperable substation control/protection systems. Because it is Ethernet-based, IEC 61850 real-time, near real-time, and ad hoc communications coexist with all of the other protocols necessary for file transfer, engineering access, diagnosis, video, telephony, etc.

The broad nature of IEC 61850 comes as no surprise to those who followed the project from its inception in 1986 when, as a part of the Integrated Utility Communication (IUC) program, EPRI launched the Utility Communication Architecture (UCA) project. Most of this work was published in 1999 as UCA2.0 (IEEE Technical Report 1550) and further used as foundation for the IEC 61850.

IEC 61850 real-time communication mechanisms are:

- GSSE Generic Substation State Event (UCA2.0 GOOSE)
- GOOSE Generic Object Oriented Substation Event per 61850-7-2
- IEC 61850-9-1 Sampled analog values over serial unidirectional point-to-point link
- IEC 61850-9-2 Sampled analog values over VLAN/priority-tagged Ethernet network

Although these four mechanisms are very powerful, it can be argued that they still lack support for some of the most demanding substation applications, such as precision time synchronization (<5 μs), line differential, and bus differential protection. It is expected that these and similar application-related issues will be resolved in the near future.

The purpose of this paper is to explain some of the lesser-known consequences of using communicated data for power system protection. It also gives working examples of using event-driven GSSE (UCA2.0 GOOSE) message exchange for fast bus trip, network reconfiguration-based breaker failure protection, and permissive transfer trip.

REAL-TIME ETHERNET

Ethernet technology was widely believed to be inadequate for mission critical, hard real-time applications, with multiple studies [4] [5] analyzing limitations of the carrier sense/multiple access (CSMA) technique. Recently, however, because of pressure from consumer-driven web-based technologies [6], Ethernet was enhanced to become a highly predictable real-time network technology [5].

This change was in part brought forward because of the pioneering design and analysis done by vendors, which warned of the shortcomings and brought about the introduction of modern high-

speed Ethernet switch technology. Following is a short list of key mechanisms behind the predictable real-time Ethernet technology.

1. 100 Mbps (with 1 Gbps becoming available) port speed
2. Full duplex port operation (IEEE 802.3x)
3. Collision-free environment
4. Priority queuing support (IEEE 802.1p)
5. Virtual LAN support (IEEE 802.1q)
6. Loss-of-link management
7. Rapid spanning tree algorithm support (IEEE 802.1w)
8. Back pressure and flow control (IEEE 802.3x)
9. IGMP layer 2/3 snooping and multicast filtering
10. Fiber-optic port interface
11. Remote monitoring, port mirroring, and diagnostic support
12. Availability of EMI-hardened, extended temperature range devices

Port Speed and Fiber-Optic Interface

Original 10 Mbps Ethernet has been virtually replaced by the upgraded 100 Mbps line interface. With the Category-5 twisted pair option, both speeds are still available and are supported automatically by the associated physical layer interface (10/100 Mbps). In the case of fiber-optic interface, the speed selection is not automatic, resulting in virtual obsolescence of the 10 Mbps option. It should also be noted that connection between 10 and 100 Mbps network segments is not seamless. It requires bridging, and it is best avoided if any real-time traffic needs to be passed between the two.

Full Duplex Operation and Collision-Free Environment

Modern switches offer a full-duplex interface capable of simultaneously transmitting and receiving remote device traffic. This capability virtually doubles the available bandwidth (200 Mbps), while eliminating the possibility of local packet collisions. Collisions involving traffic from different ports are avoided by storing (within the switch) all of the traffic that cannot be immediately forwarded. This storage keeps all of the incoming pipelines open, while making it possible to optimally schedule/combine the outgoing port traffic. Internal switch bandwidth is dimensioned to support simultaneous operation of all ports (several Gbps in the case of an 8 port 100 Mbps switch), thus maximizing the overall data throughput.

The primary function of an Ethernet switch is to establish a direct connection between the sender and the receiver (based on the individual device Media Access Controller [MAC] address). Individual packets are therefore forwarded only between the two communicating ports, without affecting the bandwidth available to other ports.

Priority Queuing

Because it is a multipurpose network, Ethernet often needs to carry vastly different types of network traffic. This is best illustrated by thinking of a power system substation application in

which mission-critical IEC GOOSE traffic (e.g., command to trip a breaker) must coexist with SCADA or device management type traffic (e.g., event oscillography retrieval). It is obvious that different messages have different delivery time requirements, making it necessary to separate the incoming traffic into different priority queues.

The priority queuing mechanism is described in the IEEE 802.1.p standard. Priority is accomplished by inserting a four-byte "tag" into the standard Ethernet frame header. Actual tag position is shown in Figure 1.

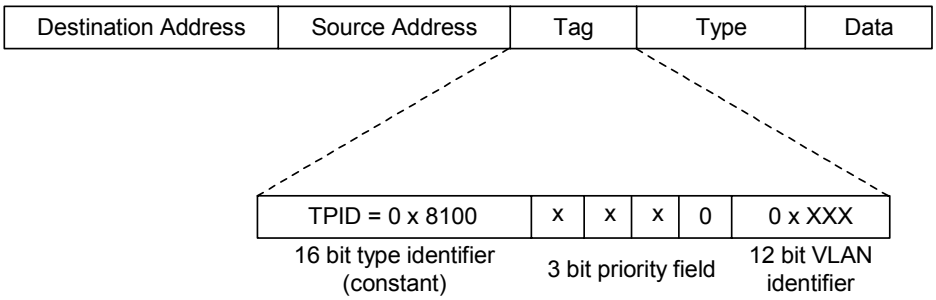

Figure 1 Layer 2 Tagged Ethernet MAC Header

The number of priority queues varies among switches, with the minimum of two needed to claim 802.1p support. Queuing strategy is usually configurable, with "strict priority" being one of the options (no low-priority messages are forwarded until all of the high-priority traffic has been processed).

Separating the traffic into priority classes makes it possible to reserve bandwidth for mission-critical protection-type applications, thus eliminating congestion and providing a delivery guarantee for the high-priority traffic. Worst-case message latency can be calculated as follows.

Let us assume that a high-priority IEC GOOSE message arrives at the switch immediately after the outgoing port has begun sending a low-priority frame. Because the outgoing port is busy, the high-priority message will have to wait. Worst-case delay can be calculated based on the maximum Ethernet frame size (1518 bytes), which in the case of the 100 Mbps Ethernet translates into 122 μs. This delay is followed by the IEC GOOSE transmission time of 24 μs (assuming a 300 byte GOOSE). In addition to this, the priority queue may already contain other high-priority messages (let us assume 10). We also need to take into account switch latency, which is normally in the order of 10 μs. The final count is shown in Table 1.

Table 1 Message Delivery Time Calculation Example

Switch latency	10 μs
Low-priority frame transmission	122 μs
10 real-time GOOSE packets	240 μs
Desired GOOSE packet	24 μs
Total	**382 μs**

It is easy to see that up to 35 IEC GOOSE messages could in theory be transmitted each millisecond.

Separation of traffic into multiple priority classes makes it possible to calculate and control the worst-case latencies encountered by the real-time traffic, within correctly designed, implemented,

and maintained networks, thus bringing back the determinism needed for real-time network operation.

Virtual LAN Support

Virtual LAN is a mechanism for partitioning the network into multiple "virtual" domains. It uses the 12-bit VLAN tag field shown in Figure 1 to divide the network into a maximum of 4096 individual domains. Virtual LAN can also be configured on an "Individual Port" basis in order to support devices without tag insertion capability.

Loss-of-Link Management

Because of the high reliability expected from power system automation devices, virtually all manufacturers have equipped their products with a redundant Ethernet port interface. This interface normally provides a "stand by" channel capable of taking over the network function in case of the primary port failure.

While detecting the loss of receiving fiber is relatively trivial (the end device notices the absence of "link" pulses), detection of the outgoing (transmit) fiber failure is somewhat more involved. In this case, the Ethernet switch will know that communication with the end device is missing, but the device will be under the impression that everything is OK because it continues to receive link pulses. As a result, the end device will not switch over to its backup port.

This problem is resolved by adding intelligence to the switch, which disables the outgoing link pulse stream after detecting the incoming link failure. Additional features may be used to enhance the switch learning capabilities immediately following a "loss-of-link" event (flushing of the MAC address table, port flooding, etc.). Exact recovery procedures are not fully standardized and remain manufacturer/product specific, thus needing verification before actual field deployment.

Rapid Spanning Tree Algorithm Support

While very powerful in terms of bandwidth and its real-time capabilities, an Ethernet network would be useless unless it were designed to ride through equipment failures and offer easy serviceability. This is accomplished by adding redundancy and using advanced network topologies. Extensive description of redundant network topologies can be found in literature [7] and will not be repeated here.

For the purposes of this discussion, it is sufficient to note that multiple communication paths will automatically be established as soon as redundancy gets introduced into the network. While multiple communication paths are desirable (in general terms) their very presence jeopardizes the OSI Layer 2 Switch-based network. Unless specifically disabled, multiple paths will result, with packets being indefinitely routed through all circular paths, leading to fast traffic buildup and complete network failure. This problem was addressed by introducing the "spanning tree" algorithm, which enables multiple switches to self-organize, discover, and temporarily disable redundant network connections. Such connections are kept in "hot reserve" and can be activated as needed. The rapid spanning tree algorithm fine-tunes the original spanning tree implementation (which could take anywhere between 1 and 3 seconds to fully restore the network), speeding it up to the 5-40 ms level.

Back Pressure and Flow Control

The carrier sense/multiple access (CSMA) technology originally used to provide network access arbitration and collision detection appears to be unnecessary in the "collision-free" Ethernet switch environment. This appearance is deceptive. In the Ethernet switch-based environment, CSMA is being used as a last resort (emergency) technique capable of providing "back pressure" (reducing traffic flow) in rare cases when overall traffic exceeds individual switching capabilities.

IGMP Layer 2/3 Snooping and Multicast Filtering

While the basic switching mechanism is very effective in dealing with the directly addressed frame traffic, its benefits disappear when exposed to "broadcast" and "multicast" frames.

The multicast concept is crucial for power system applications in which a given analog value, state change, or command may have to be communicated to several peers at the same time. Instead of multiple individually addressed messages, a single multicast message is sent to a switch, which would normally forward it to all outgoing ports. Receiving devices are simply configured to listen to a particular multicast address, thus making it possible to disregard the unwanted network traffic.

Because of indiscriminate output port flooding, extensive use of multicast traffic may prevent the assembly of larger Ethernet-based substation networks. Partitioning multicast traffic and limiting it to individual "Multicast Domains" can optimize system performance.

Partitioning can be achieved in different ways, and IGMP (Internet Group Multicast Protocol) is one of the most efficient methods. IGMP was originally developed for router-based communications. It allows individual Ethernet devices to form, join, and leave various multicast groups at will.

Strictly speaking, IGMP is an OSI Layer 3 function, which has been extended to Layer 2 switching devices by adding the "listen in" or "snooping" functionality. The Ethernet switch simply listens in on an IGMP conversation and configures itself accordingly to route multicast packets to the currently subscribing multicast group members. Multiple groups are easily supported with dynamic group membership management.

While very powerful, IGMP snooping requires the presence of higher-level IP protocols (Layer 3 IP address field) and cannot be directly applied to IEC 61850 GSSE, GOOSE, or sampled analog value type messages.

A theoretical example of multicast domain partitioning showing multicast domains that are conveniently arranged to reflect the individual protection zone coverage is given in Figure 2.

Remote Monitoring, Port Mirroring, and Diagnostic Support

Given the scalable nature, speed, and complexity of modern Ethernet networks, it is easy to see how network management can grow to become a major obstacle. A variety of standard tools are available to accomplish this task.

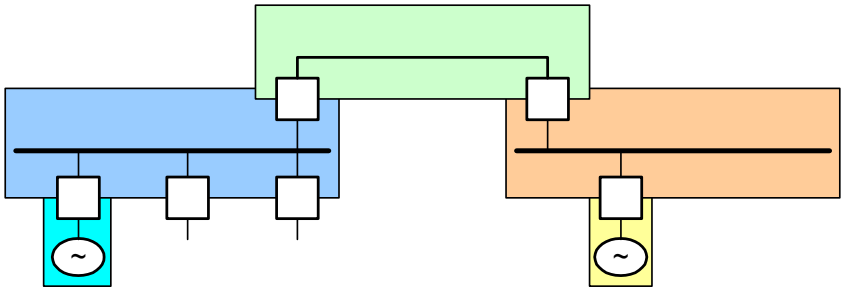

Figure 2 Simple Multicast Domain Partitioning Example

Power System Protection, Automation, and Ethernet Network Limitations

It would be inappropriate to end this discussion without taking a look at the issues and requirements associated with real-time Ethernet network technology.

Very high availability achieved through network equipment redundancy is associated with several undesirable side effects:

- Possibility of delayed frame reception
- Temporary loss of network function (5-40 ms) due to reconfiguration
- Engineering/planning mistakes
- Network congestion
- Network system maintenance related outages

Any power system application relying on Ethernet networks for data exchange must be designed to effectively cope with this environment. Once more we are faced with a decades-old dilemma of having to provide **reliable automation and protection using inherently unreliable communication channels.** This can be accomplished by carefully designing conventional automation and protection systems based on locally measured voltage and current values.

For protection, standard overcurrent elements, time-overcurrent coordination techniques, distance protection, harmonic restraint, under-/overfrequency (voltage), transformer differential, etc. should be used to provide basic system protection. Once the system is protected in a conventional fashion (using locally measured data), it is desirable to use communicated data from remote nodes to improve fault selectivity, increase speed of operation, or add additional intelligence made possible by global situation awareness.

In an Ethernet network-based environment, locally derived conventional protection becomes a reliable backup mechanism used to supplement the “high performance,” communication network-based, functionality. When communication-enhanced protection is properly combined with reliable conventional backup, the resulting system offers exceptional availability and resiliency to multiple system failures.

While the above approach is not new, what changed is the ease and magnitude of data sharing possible in the Ethernet network environment. Furthermore, the new network environment allows for continuous communication system monitoring, thus making it possible to optimize the protection device decision-making process based on the actual amount of data available at any given time.

For example, two IEDs protecting a transmission line by periodically exchanging directional data at a rate of 4 ms can track the arrival of remote end messages. In case of the communication

system disruption, communicating devices can instantaneously switch over to reliable distance-based backup. The process can be repeated for every individual message, thus providing very fine time granularity and seamless coordination between the primary (communication-based) protection and the reliable conventional backup.

The above guidelines for the design of Ethernet network-enhanced protection systems can be summarized as follows:

- Network-enhanced protection systems must be built on top of (supplemented by) a reliable local backup.
- Any loss of communication capability must be reliably detected and addressed, resulting in gradual, predictable, and coordinated performance degradation.
- Message error detection and control must be rigorous and capable of detecting all possible message corruptions.
- Network-based communications must be continuously monitored.
- Continuous data exchange is preferred over the event-driven model. This approach makes it possible to establish both the health of the communication channel and the health of the peer IED participating in the message exchange.
- Reliance on communication time delays and message arrival time coordination should be avoided whenever possible. Multiple messages may be exchanged in order to guarantee operational correctness and to avoid complex race conditions.

It should be noted that attempts to save network bandwidth by using event-driven message exchange are ill conceived by optimistically assuming that the message will be able to traverse the network during periods of high traffic congestion (substation fault). The biggest problem with the event-driven model is its inability to reliably detect the message loss. When it comes to power system protection, it is most productive to reserve the required bandwidth ahead of time (e.g., by allocating 20 percent for high-priority network traffic), and to use this bandwidth continuously, thus providing real-time system monitoring and instantaneous failure detection.

In short, if the message is important enough to be sent at the time of crisis, it should be important enough to be sent continuously, thus providing reliable channel monitoring. The information about message absence is often as valuable as the message itself, making it possible to adapt the protection system response to the current communication network state.

In order to support real-time protection over Ethernet, substation network infrastructure needs to satisfy the following minimum requirements:

- Ethernet hubs should not be used, and they should be replaced by Ethernet switches.
- All Ethernet switches need to be managed.
- Every switch must support 100 Mbps full duplex port operation (10 Mbps support is optional).
- Priority queuing, virtual LAN, rapid spanning tree, and IGMP snooping functionality should be supported.
- High-priority network traffic should be allocated to power system protection and high-speed automation. High-priority traffic volume must be carefully planned, managed, and monitored throughout the lifetime of the installation.
- Redundant network architecture is highly encouraged.
- All Ethernet switches must be rated for operation in the substation environment.

- The Utility's Information Technology (IT) department should be involved early on in the project.
- Network security (especially external access to the substation LAN) must be addressed at the planning stage and properly managed throughout the lifetime of the installation.

APPLICATION EXAMPLES

While most of the described IEC 61850 real-time communication mechanisms are still being integrated into products, IEC GSSE message (UCA2.0 GOOSE) has been available for over three years and is supported by all major manufacturers. It is interoperable, has been extensively tested, and can be applied in real-life installations. The remainder of this paper concentrates on showing simple examples of IEC GSSE message capabilities.

As already stated, IEC GSSE message is equivalent to the UCA2.0 GOOSE. It should not be confused with IEC 61850 GOOSE, which represents an enhanced superset capable of transferring complex data structures with an arbitrary combination of characters, binary values, integers, floating point numbers, etc. Following is a short list of the IEC GSSE message properties:

- IEC GSSE message is used to transfer 96 binary variables (states). If required, this number may (depending on the implementation) be extended up to a total of 512 binary variables.
- IEC GSSE message is generated in response to a state change (system event).
- In the absence of a state change, IEC GSSE message will be generated at preset time intervals (IEC GSSE refresh rate, most commonly 1 s).
- There is no standardized acknowledgment mechanism.
- The standard implementation requires sending multiple messages in fast succession to increase the likelihood of message delivery. An exponential back-off mechanism is used to increase time between messages.
- IEC GSSE message is normally sent using a multicast group address.
- IEC GSSE message is not routable. It can be bridged between different OSI Layer 3 domains (WAN).

The following examples illustrate the use of GSSE (UCA2.0 GOOSE) messages for power system protection. The examples are intended to illustrate good protection practices [9] consistent with the general guidelines explained in earlier parts of the paper, while at the same time addressing inherent limitations associated with the IEC GSSE message definition. Application examples are based on logic equations described in [10].

FAST BUS TRIP

Substation bus protection is most often accomplished by using dedicated differential protection. This approach offers exceptional speed and very high selectivity, but is associated with relatively high cost. While cost may not be an issue for high-voltage switching and generator substations with multiple sources attached to the same bus, it may become prohibitive in cases of simple distribution voltage substations with one source and radially fed loads. It is in these lower-voltage distribution substations that communications-assisted "fast bus trip" often replaces the bus differential.

Typical distribution substation layout is shown in Figure 3. The substation has three radially fed feeders (as indicated by the three breakers located below the bus) and one source breaker (located

above the bus). Fast bus trip protection is accomplished by bringing the feeder relay status back to the main bus relay that is in charge of the source-side breaker. In case of a feeder fault, both the affected feeder relay and the bus relay will detect the overcurrent condition. Based on the fault indication supplied by the feeder relay, the bus relay will back off, allowing the feeder relay to clear the fault based on a previously set protection strategy (most often inverse-time overcurrent).

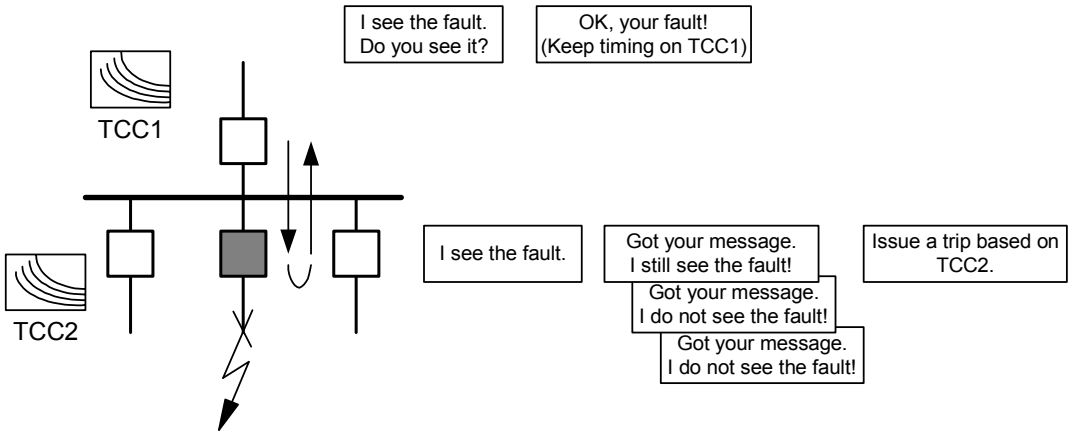

Figure 3 Feeder Fault Scenario

The bus fault-clearing scenario shown in Figure 4 is somewhat more interesting. In this case, the fault is seen only by the bus relay. The bus relay must first be able to verify that none of the feeder relays is able to see the fault before issuing the trip command.

While very simple, the fast bus-tripping scheme is intimately dependent on the method used to bring the feeder relay overcurrent element status information to the bus relay. In conventional installations, this is often accomplished by hardwiring a set of output contacts or by contact state mirroring through dedicated serial communication channels. In both of these cases, the states are being brought in and refreshed continuously (approximately every 4–10 ms).

When a fast bus trip is implemented using IEC GSSE messages, it is necessary to note that IEC GSSE conveys only a "status change." This means that in the above bus fault example, the need to trip the bus breaker will be indicated by total silence (lack of GSSE messages) from the feeder relays. As a consequence, the simple "state change" communication-based approach cannot distinguish a legitimate trip situation from the Ethernet communication system failure.

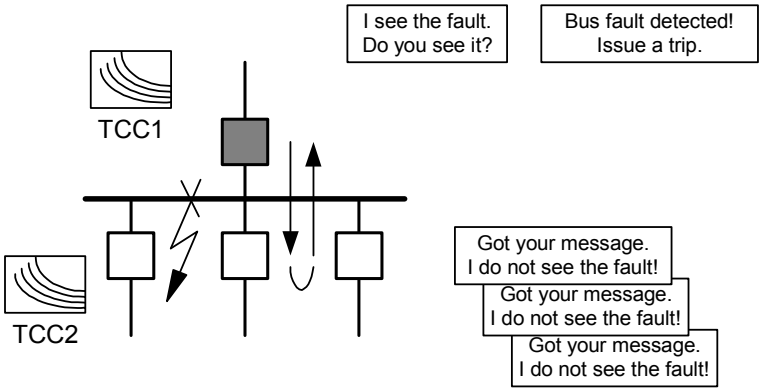

Figure 4 Bus Fault Scenario

Bus and feeder relay coordination is normally established by using time-current coordination (clearing times > 400 ms) as indicated in Figure 3 and Figure 4 with time current curve symbols (TCC1, TCC2). Faster fault clearing times can be accomplished by using a challenge/response scheme proposed in Figure 3 and Figure 4. In this case, the feeder relays are programmed to report two different state changes. First is the state change of the overcurrent element. The second change is the state change of the received IEC GSSE message. In addition to that, the bus relay is also programmed to emit a IEC GSSE message, reflecting the change of its own overcurrent element.

Message exchange for a feeder fault scenario is shown in Figure 3. Conversation begins with both the bus relay and the affected feeder relay almost simultaneously reporting, "I see the fault." Upon reception of the message from the bus relay, all feeder relays report their states back to the bus relay, which disables its time-overcurrent function and allows the feeder relay to clear the fault.

Message exchange for a bus fault scenario is shown in Figure 4. Conversation begins with the bus relay reporting, "I see the fault." Upon reception of the message from the bus relay, all feeder relays report their state back ("I do not see the fault"). As soon as the messages are received, the bus relay has positive confirmation of the fault location and can clear the bus.

Table 2 Fast Bus Trip Relay Settings (programmable logic example)

	Bus Relay	**Feeder Relay 1**
Tx. Goose ID	GOOSE_B	GOOSE_1
Rx. Goose ID	GOOSE_1 GOOSE_2 GOOSE_3	GOOSE_B
Goose Multicast MAC Address	01-30-A7-00-10-8A	01-30-A7-00-10-8A
Goose Output Mapping	CCOUT1 := 50P1	CCOUT1 := 50P1 CCOUT2 := CCIN01
Goose Input Mapping	CCIN01 1:33 (feeder1 50P1) CCIN02 1:34 (50P1 echo1) CCIN03 2:33 (feeder2 50P1) CCIN04 2:34 (50P1 echo2) CCIN05 3:33 (feeder3 50P1) CCIN06 3:34 (50P1 echo3)	CCIN01 1:33 (upstream 50P1)
Protection Logic	PSV60 := NOT CCIN01 AND CCIN02 AND NOT CCIN3 AND CCIN4 AND NOT CCIN5 AND CCIN6 AND 50P1	
Trip Logic Mapping	PSV60 OR 51S1T	51S1T
CCOUT1 – Communication card output point 1 mapped to transmitted IEC GOOSE CCIN01…06 – Communication card input points 1 through 6 mapped from received IEC GOOSE PSV60...61 – Protection logic variables 60 and 61 51S1T – Time-overcurrent element 1 timeout		

The example in Table 2 illustrates the IEC GSSE-based handshake mechanism for interrogating a state of an otherwise unresponsive peer. With the settings given in Table 2, the logic typically

achieves bus trip times between 16 to 25 ms. Instantaneous overcurrent element coordination is achieved using IEC GSSE message time delay and by setting the bus overcurrent element pickup greater than the feeder OC element pickups. It is important to note that in Table 2, Table 3, and in Table 4, "Goose" indicates UCA GOOSE or IEC GSSE, while MAC refers to the media access control address.

In contrast to the handshake-based approach described above, reference [2] proposes the use of a definite-time overcurrent strategy. According to [2], the bus relay is set with a time delay, which is only long enough to give the feeder relays time to report they have detected the fault. The main drawback of this approach is that there is no way to distinguish between the communication message loss and the absence of the feeder fault. When implemented using IEC GSSE messages, the traditional definite-time overcurrent method is prone to misoperation because a simple communication message loss can lead to clearing of the entire substation bus.

BREAKER FAILURE PROTECTION

Breaker failure protection is a last resort, timer-driven scheme intended to coordinate upstream device operation necessary to clear a fault in situations when a downstream protection device issues a trip command, but its associated breaker fails to clear the fault within a prescribed breaker failure time interval (typically 7 to 15 cycles). The breaker failure trip signal may have to be communicated to as little as one adjacent device, or as many relays/intelligent breakers as necessary to clear the fault. Because it is a multicast message, IEC GSSE is naturally suited for the task.

Table 3 shows a simplified example of a breaker failure protection system applied on a two-breaker system. While these settings are deceptively simple, actual implementation using multiple breakers will have to take into account additional logic necessary to determine which devices need to respond to the breaker failure signal.

The above example shows that the breaker failure function that was once centralized within a single "breaker failure relay" can now be distributed among multiple IEDs. Depending on the implementation, the breaker failure timer can now be implemented within the primary protection device, within the backup protection device, or distributed among multiple devices on the network.

Table 3 Breaker Failure Example Settings

	Monitored Device	**Backup Devices**
Tx. Goose ID	GOOSE_1	GOOSE_2
Rx. Goose ID	GOOSE_2	GOOSE_1
Goose Multicast MAC Address	01-30-A7-00-10-8A	01-30-A7-00-10-8A
Goose Output Mapping	CCOUT1 := FBF1	CCOUT1 := FBF1
Goose Input Mapping	CCIN01 1:33 (remote breaker failure signal)	CCIN01 1:33 (remote breaker failure signal)
Breaker Failure Trip Logic Mapping	FBF1 OR CCIN01	FBF1 OR CCIN01
FBF1 – Circuit breaker 1 breaker failure CCOUT1 – Communication card output point 1 mapped to transmitted IEC GOOSE CCIN01 – Communication card input point 1 mapped from received IEC GOOSE		

PERMISSIVE OVERREACHING TRANSFER TRIP

Permissive overreaching transfer trip (POTT) [9] is a very popular communications-assisted scheme capable of providing fast and secure transmission line protection. It was originally applied with carrier-based communication channels and has been successfully adapted to modern digital communications.

The basic POTT scheme operating principle is illustrated in Figure 5. It is easy to notice that Breakers 2 and 3 can be tripped whenever their associated relays simultaneously see a fault in the forward-looking direction (Zone 2). Zone 3 must be configured to look in the reverse direction and needs to reach further than the overreaching Zone 2 from the remote line terminal.

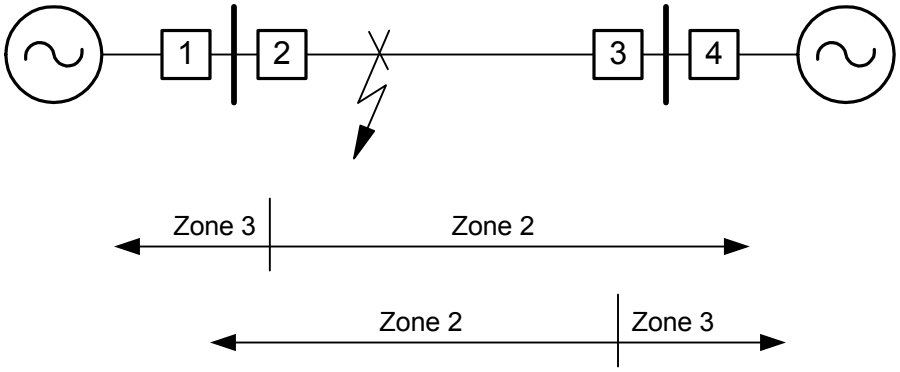

Figure 5 Basic POTT Scheme With Associated Zones of Protection

Logic required for POTT scheme operation is often prebuilt and is easily accessible through modern microprocessor-based relay settings menus. Once configured, the POTT logic will typically generate a communication signal (marked KEY in Table 4 and Figure 6), which is properly conditioned and ready to be sent to the remote terminal. Typical KEY signal logic is shown in Figure 6.

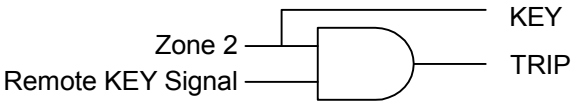

Figure 6 Basic POTT Logic

Once received on the remote end, the KEY signal is compared with the local zone element information. The relay issues a trip if both local Zone 2 elements and the KEY signal from the remote end are simultaneously active.

The use of IEC GSSE message for a POTT scheme is relatively straightforward, as illustrated in Table 4. The biggest challenge lies in the fact that IEC GSSE message is not routable. Because the POTT scheme normally spans two different substations, it is also necessary to make sure that the IEC GSSE message can be reliably delivered over large distances. Depending on the distance between the substations, this can be achieved by either expanding a single Ethernet network to span both substations (single-switched Ethernet domain), or more commonly by using routers to partition the system into multiple subnetworks. Because IEC GSSE messages are not routable, routers must be manually configured to "tunnel" the IEC GSSE-specific multicast traffic between the two networks.

Permissive overreach transfer trip belongs to a wider group of communications-assisted directional tripping schemes. While very popular for line protection applications, it can very

effectively be used to protect sensitive industrial loads. Figure 7 shows one such application in which directional communications-assisted tripping can be used to reliably isolate faults and provide fast restoration of service (within several cycles) to the rest of the network.

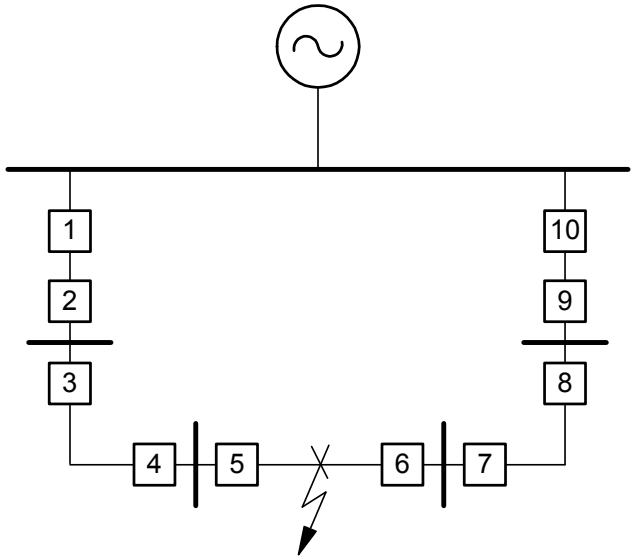

Figure 7 Industrial Park Protection Concept Using POTT Scheme

Table 4 Permissive Overreach Transfer Trip Example Settings

	Device 1	Device 2
Tx. Goose ID	GOOSE_1	GOOSE_2
Rx. Goose ID	GOOSE_2	GOOSE_1
Goose Multicast MAC Address	01-30-A7-00-10-8A	01-30-A7-00-10-8A
Goose Output Mapping	CCOUT1 := KEY	CCOUT1 := KEY
Goose Input Mapping	CCIN01 1:33 (Remote end POTT)	CCIN01 1:33 (Remote end POTT)
Enable Communication Scheme	POTT	POTT
Protection Logic	PT1 := CCIN01	PT1 := CCIN01
Communications-Assisted Trip Logic	TRCOMM := M2P OR Z2G	TRCOMM := M2P OR Z2G
KEY – Transmit permissive trip signal CCOUT1 – Communication card output point 1 CCIN01 – Communication card input point 1 PT1 – General permissive trip signal received M2P – Zone 2 phase distance element Z2G – Zone 2 ground distance element		

CONCLUSION

This paper presents opportunities for enhancing power system automation through the use of real-time Ethernet. It explains the latest international standards and mechanisms available to power system engineers. It explains advantages and pitfalls associated with the technology and gives guidance for the design of reliable communications-assisted protection schemes, including three

application examples demonstrating the use of IEC GSSE/UCA2.0 GOOSE messages for power system protection purposes.

It should be noted that none of the applications presented in this paper may individually be able to justify the investment of equipping the substation with Ethernet network capability. However, once the Ethernet has been justified, a GSSE message offers a preferred method for exchange of real-time status information among multiple protection devices. IEC GSSE message can be used to simplify substation wiring, reduce installation cost, and enhance overall protection system performance. When properly applied, IEC GSSE message offers a powerful new tool in the power system protection and automation engineer's toolbox.

REFERENCES

[1] A. Apostolov, B. Muschlitz, "Practical Realities and Future Potential – Implementation Benefits of DNP3 and IEC61850," DistribuTECH Conference and Exhibition, January 2004.

[2] IEEE PSRC, WG H5, "Application of peer-to-peer communications for protective relaying," web published report, available at http://www.pes-psrc.org/h/H5doc.zip.

[3] IEEE PSRC, WG H6, "Application Considerations of UCA2 for Substation Ethernet Local Area Network Communication for Protection and Control," web published report, available at http://www.pes-psrc.org/h/.

[4] T. Skeie, S. Johannessen, C. Brunner, "Ethernet in Substation Automation," IEEE Control Systems Magazine, June 2002.

[5] M. P. Pozzuoli, "Ethernet in Substation Automation Applications – Issues and Requirements," DistribuTECH Conference and Exhibition, January 2004.

[6] O. Holmeide, T Skeie, "VoIP Drives Real Time Ethernet," available at http://www.ontimenet.com/pdfs/VoIP drives realtime Ethernet.pdf.

[7] M. Galea, "Rapid Spanning Tree in Industrial Networks," available at http://www.ruggedcom.com/Pdf/Wpapers/Rapid Spanning Tree in Industrial Networks.pdf.

[8] M. Feltis, J. Kumm, "SEL Application Guide AG94-11, Applying the SEL-501 Relay for Fast Bus Trip and Simple Bus Breaker Failure Protection," Schweitzer Engineering Laboratories, Inc.

[9] A. Guzman, J. Roberts, K. Zimmerman, "SEL Application Guide AG95-29, Applying the SEL-321 Relay to Permissive Overreaching Transfer Trip (POTT) Schemes," Schweitzer Engineering Laboratories, Inc.

[10] "SEL-421 Relay User's Guide," Schweitzer Engineering Laboratories, Inc., available at http://www.selinc.com/instruction_manual/421/421_UG_20040602.pdf.

BIOGRAPHIES

Veselin Skendzic (M '87, SM '03) earned his BSEE from FESB, University of Split, Croatia, in 1983, M.Sc. from ETF, Zagreb, Croatia, in 1990, and his Ph.D. from Texas A&M University, USA, in 1994. Veselin has over 20 years of experience in electronic circuit design, has lectured at FESB, and has spent over 14 years working on power system protection related problems.

Veselin spent ten years at Cooper Power Systems, where he helped establish the protective relay product line. At the beginning of 2004, Veselin joined Schweitzer Engineering Laboratories in Pullman, Washington, where he is currently a senior research engineer. Veselin is a senior member of IEEE, has authored multiple technical papers, has five patents, and has contributed to four IEEE standards. Veselin is an active participant in IEEE Power System Relaying Committee (PSRC) activities.

Armando Guzmán (M '95, SM '01) received his BSEE with honors from Guadalajara Autonomous University (UAG), Mexico, in 1979. He received a diploma in fiber-optics engineering from Monterrey Institute of Technology and Advanced Studies (ITESM), Mexico, in 1990, and his MSEE from University of Idaho, USA, in 2002. He served as regional supervisor of the Protection Department in the Western Transmission Region of the Federal Electricity Commission (the electrical utility company of Mexico) for 13 years. He lectured at UAG in power system protection. Since 1993 he has been with Schweitzer Engineering Laboratories in Pullman, Washington, where he is presently a Fellow Research Engineer. He holds several patents in power system protection. He is a senior member of IEEE and has authored and coauthored several technical papers.

20041114
TP6188-01