

IEEE (ANSI) Device Number 16 – Ethernet Switches and Routers

Eric A. Udren
KEMA Consulting, Pittsburgh, PA

In electric utility and industrial applications, Ethernet local area networks (LANs) and wide area networks (WANs) are being used for message transmission to carry out high-speed control and protection. A prime example for utilities is the use of IEC 61850 GOOSE messages in a substation Ethernet LAN environment to transmit a primary or backup trip commands from one relay to another without conventional wiring. These networks are widely used for control of power apparatus via SCADA or by local operators, even if IEC 61850 is not in use.

The Ethernet networks in substations comprise wired connections or optical links connecting relays and other IEDs in a LAN based on a managed Ethernet switch, described in the paper. The switch is in fact an elaborate message-processing computer with a list of settings that impacts how the protection messages are sent from one relay to another.

Furthermore, these substation LANs are connected to the utility enterprise WAN via Ethernet routers, sophisticated message processing computers also described below. As inter-substation Ethernet messaging is used for control and protection, the routers and the WAN also become protective relaying auxiliary devices and channels. Sprinkled among the switches and routers may be cyber security functions including firewalls, encryption function blocks, and VPN clients.

IEEE C37.2 is the familiar standard for device numbers of protective relaying functions, sometimes referred to as ANSI device numbers. C37.2-1996 is having its latest revision at time of writing. A *proposed* change, favorably received so far by the joint PSRC-SC C37.2 Revision Working Group, is to assign the formerly unused Device Number 16 to data communications devices in substation protection and control (P&C) schemes, including serial or Ethernet communications networks carrying protective relaying traffic. The proposal includes a scheme of added letters that identify the particular type of data communications function that the box performs, as described below.

While this paper shows examples of use, note that the standard development is still in process and that specifics may change before an agreed standard revision is accepted and issued by IEEE.

The real message for the present protective relaying audience is that many Ethernet communications devices have become critical relaying components appearing in drawings and documentation for today's protective relaying and substation control schemes. Ethernet local area network (LAN) based protection and control schemes using IEC 61850 GOOSE messaging depend on the proper setting and operation of Ethernet switches and routers for high-speed primary or backup relaying, or breaker lockout after a backup trip, to take place. Relay engineers will need to learn the basics of what these communications devices do and how to use them. They can be regarded as the new generation of auxiliary relays.

Ethernet switches and routers installed on relay panels in hostile substation environments are descended from equipment widely used in IT networks. Accordingly, the IT departments at many

utilities have taken control of the selection, application, management, and setting of switches and routers. In some cases, there is a lack of mutual understanding between the protection/control designers and the IT experts about the role of these devices, how they are to be managed, and by whom.

This paper describes the basic design, purpose and functionality of these communications devices of proposed IEEE Device Type 16 in substation LANs.

IEEE C37.2 Device Numbers

IEEE C37.2-1996, *IEEE Standard Electrical Power System Device Function Numbers and Contact Designations* [1], provides a shorthand notation for relaying and control functions. This notation has been familiar to protection engineers since AIEE Standard 26 was issued in 1928. The 1996 standard was reaffirmed in 2001. The 2007 revision project is the ninth for this document, which remains vibrant and has seen important additions even in recent years. IEC Technical Committee 95, which deals with relays, is interested in this Standard in light of its international use. Table 1 shows some of the most commonly used protective relay function numbers.

11	Multifunction device - contains other numbers as appropriate (new in 1996 edition).	55	Power factor relay
21	Distance relay	59	Overvoltage relay
25	Synchronizing or synch-check relay	62	Time delay stopping relay
27	Undervoltage relay	67	Directional overcurrent relay
32	Directional power relay	68	Blocking relay
37	Undercurrent or underpower relay	78	Phase angle or out-of-step relay
43	Manual selector	79	Reclosing relay
46	Reverse-phase, phase-balance, or negative-sequence current relay	81	Frequency relay
47	Phase-sequence voltage relay	85	Carrier or pilot relay
49	Thermal relay	86	Lockout relay
50	Instantaneous overcurrent relay	87	Current differential relay
51	Time-overcurrent relay	89	Power disconnect switch
52	Power circuit breaker	94	Auxiliary tripping relay
		101	Breaker control switch
Add suffix letters and numbers - e.g.:			
67N is neutral (ground) directional overcurrent relay			
21P-1 is zone 1 phase distance relay			

Table 1 – Commonly used device numbers from ANSI/IEEE C37.2-1996

The 1996 update brought the addition of Device 11, multifunction device, to be used for a relay that combines 3 or more functions having their own device numbers. This met the need for efficient shorthand diagramming of multifunctional microprocessor relays. Annex A of the standard shows two examples of how device number 11 is used, and Figure 1 here shows examples similar to those in the Annex. The upper example shows the empty-box method, and the lower example is the full-box version of Device 11.

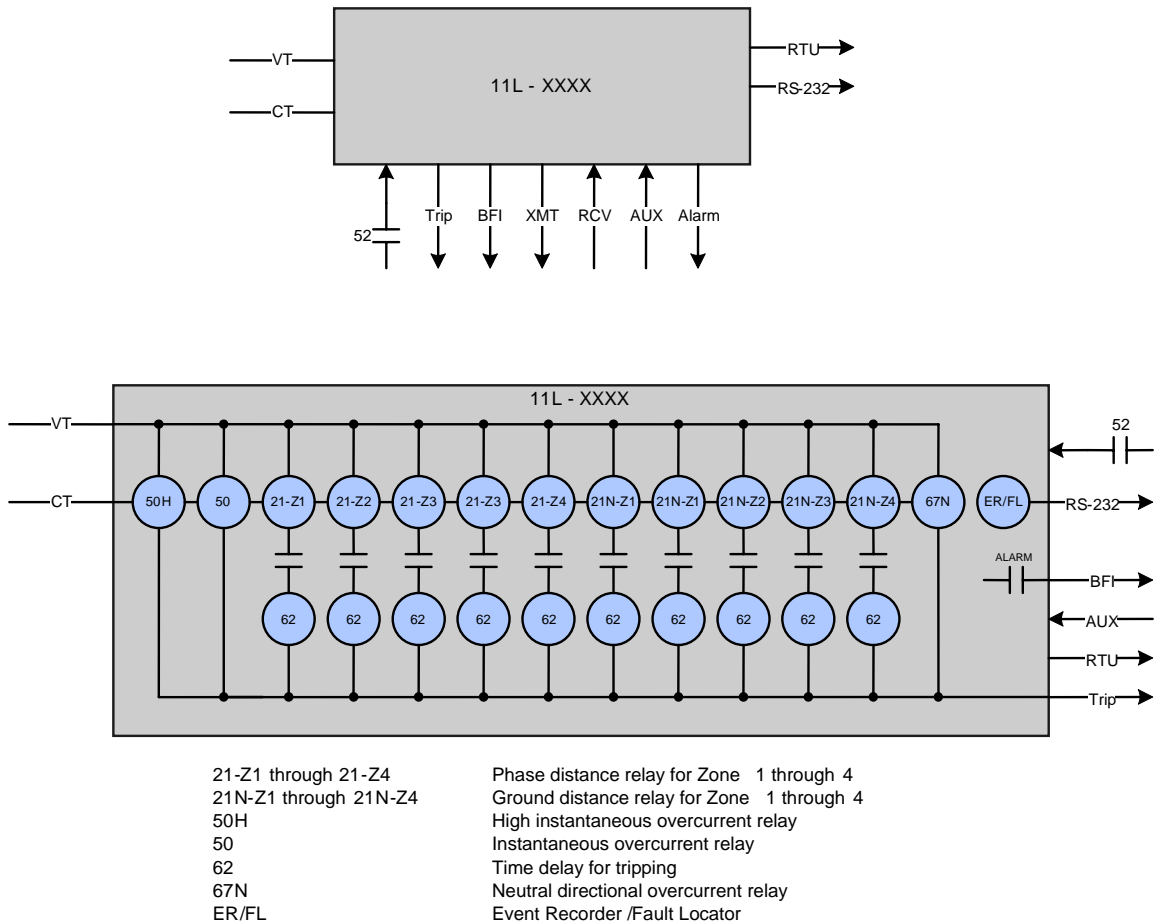


Figure 1 – Device 11, Multifunction Relay, Empty-Box and Full-Box Examples

As an aside to the theme of the present paper, we point out that there are seven two-digit device numbers in C37.2 that are obsolete (perhaps going back to 1928) and not likely used in any recent drawings. The working group is surveying the industry to confirm that these device numbers can be reassigned to new functions. Device 16 is available for use on data communications devices as proposed below, but it was the last unassigned two-digit number. There are other new relay-related functions that would be well served by their own new numbers, such as phasor measurement units (PMUs) and PMU implementations within relays, or substation time base devices like GPS clocks with IRIG-B outputs. At the end of the paper is contact information for the Chairman of the Working Group that is in the process of revising C37.2-1996.

Communications Systems and Configurations for Substation P&C Schemes

With the first-generation microprocessor relays in the late 1980s, protection engineers for the first time had access to fault and relay operating information by data communications. A plethora of technical papers at regional relay conferences and elsewhere over the last 18 years have discussed relay communications port connections for data access, and use of the data, setting, and control capability they provide.

If the communications port is only used by a technician or engineer who visits the substation and plugs in a laptop computer, the communications capability does not add any new devices to the

basic relaying and control panel. However, most utilities have connected the ports to communications devices that integrate multiple relays and other intelligent electronic devices (IEDs), to make the data remotely accessible.

To explain the roles of communications devices that are being designed into substation P&C schemes, we present the following sequence:

- Review of familiar data communications formats found in substations, and commonly used communications devices associated with each.
- Introduction of the IEEE Device 16 nomenclature.
- Examples of styles of substation communications integration using devices to which we apply Device Number 16.
- More details on Ethernet devices and applications in protection.

The paper concludes with an assessment of organizational issues related to the use of Ethernet in substations.

Physical Communications Layers

Many relay conference papers on data communications have explained how the process of data communications is broken into seven layers, for clear understanding and consistent design. The seven layers also allow for updating of parts of the communications system design while retaining other parts that continue to be useful. In particular, technology for the lower layers advances rapidly and we would like to update it frequently. We would like to do this while keeping the upper layers, which are designed for particular utility applications and which would be difficult and expensive to recreate. Table 2 summarizes the seven layers of the OSI model. In this paper, we focus on layers 1 through 3 only.

Layer	Name	Function
7	Application	Meaning of the data (utility user specifics)
6	Presentation	Building blocks of data and encryption for security
5	Session	Opening and closing specific communications paths
4	Transport	Error checking
3	Network	Determining the data paths within the network
2	Data Link	Data transmission, source & destination, checksum
1	Physical	Signal levels, connections, wires, fiber, wireless

Table 2 – 7 Layer OSI Communications Stack

Most substation communications integration is based on one or more of the following communications layers. Relays and intelligent electronic devices (IEDs) have at least one port supporting one of the following. More recent multifunctional relays and IEDs support multiple interface types and multiple communications connections. There do exist less widely used or vendor proprietary communications networks that we do not treat here.

RS-232 serial communications – a point-to-point or link serial data exchange using common-mode signals (a signal lead in each direction, and a common or ground return conductor). This is the Layer 1 physical exchange supported by ubiquitous PC serial ports and free-standing mass-

market modems for telephone circuit communications. A link supports data exchange only between two devices.

Common RS-232 communications devices:

1. Modem - for telephone circuit interface. This includes encrypting modems for cyber security of relay communications.
2. Link converter – allows interface of an RS-232 port with wireless connections, optical fibers, or virtual connections over other network types such as RS-485 and Ethernet described below. Eliminates the bulky, distance limited, and noise-vulnerable standard serial cable.
3. Serial port switching device - if more than two devices are to be connected, each needs its own port and some sort of switching among the ports is needed. This gives a local or remote user a single point of access that can pass through the link connection to any of the connected devices.
4. Communications processor – a dedicated computer with multiple ports to which RS-232 devices are individually connected. The processor exchanges data with each device for gathering a data base and presenting it conveniently to local remote users. It includes the basic switched pass-through access of (3).

RS-485 serial communications – a networked or multidrop serial data exchange using differential mode signals (two signal conductors to which the data stream is applied in opposing polarities; neither conductor is grounded). This signaling gives better immunity to electrical interference, higher data rates, and longer wiring runs than for RS-232. The networked connection means that a connected relay or IED can send data that can be heard by all the others on the network at the same time. Thus, a single network conductor is routed around the substation to connect all the communicating devices. The rules for when devices can talk or listen on the multidrop network are managed by higher layers in a selected protocol such as DNP3.

Common communications devices:

1. Link converter - supporting replacement of the RS-485 standard cable with wireless connections, optical fibers, or virtual connections over other network types such as Ethernet described below.
2. Communications processor – as described above, but with RS-485 ports so that the RS-485 networked devices can be integrated with RS-232 links and/or other types of networks including Ethernet described below.

Ethernet communications – a networked or multidrop data exchange using a standard message packet format, and a variety of signaling methods with much higher data rates than are used in RS-232 or RS-485 communications. Layers 1 and 2 are standardized by the choice of Ethernet. Most readers recognize Ethernet as the basis of information technology (IT) networks in all business enterprises and many homes. Ethernet implementations packaged in standard electronic chip sets accept a string of data bytes from higher-level computer or relay application program, frame the string in an Ethernet data packet, transmit it on the network, and perform the reverse processing for received data packets passed back to higher-level applications. The most common Ethernet physical layers are:

1. Coaxial cable with modulated high-frequency carrier, and a raw data capacity of 10 Megabits per second (Mbps). It is a true multidrop network in which all the communicating devices are tapped to the coax cable. All connected devices can hear if any sends a message. If two devices try to send data packets at the same time, both

detect the collision of messages, stop transmitting, and back off to take turns sending. As the network becomes busy (traffic load above 30% of raw capacity), the number of collisions increases dramatically, and the efficiency for data communications drops. Throughput times for messages increase unpredictably. *Networks based on coaxial cable are obsolete.*

2. Bidirectional twisted-pair connections to a repeating central hub. Each twisted-pair wired connection is an electrical link. The twisted-pair link is called 10Base-T for 10 Mbps, or 100-BaseT for 100 Mbps. The hub in the center is listening to all the links in parallel. It repeats any received signal back to all the other devices, so that the connection works like the coaxial cable multidrop network. However, the electrical connections and network installation are simpler and less expensive. Collisions, retransmissions, and loading issues are the same as with the coaxial cable version of Ethernet. *Networks based on Ethernet hubs are obsolete.*
3. A star configuration of 10Base-T or 100Base-T links as in (b) above, but with the hub replaced by an *Ethernet Switch*. Switches are intelligent interconnecting devices that demodulate, parse, store, and queue message packets from and to each link, rather than just repeating them. Switches handle each incoming packet stream separately, and sends each to other network devices in a sequence that eliminates all collisions and allows the networked connection of devices to perform to its theoretical capacity. Newer equipment also supports links operating at speeds of one Gigabit per second. There is much more to say about what switches do – they are described in another section below.
4. A network configuration as in (c) above, but with the twisted pair links replaced by optical fiber pairs, described as 10 Base FL or 100 Base FL. There are also Gigabit fiber links. Networks based on optical fiber pairs are immune to electrical interference, and are thus useful in substations, especially if the network is carrying protective relaying or apparatus control traffic.

An Ethernet local-area network (LAN) is a domain of connected devices that directly address and exchange message packets. Beyond this, Ethernet messages can be processed with elaborate schemes of recoding of addresses, and the readdressed messages can be forwarded in an arbitrarily large interconnection of communicating devices. This address recognition and translation capability facilitates the Internet, as well as wide-area networks (WANs) used by larger business enterprises to interconnect all users while isolating specific resources to subgroups of users that need access. LANs in utility substations may be connected directly to some part of the utility WAN through an address translation computer called an *Ethernet router*, described briefly further below.

The term “serial” is widely applied to RS-232 links and RS-485 networks to describe the bit-by-bit transmission of data on a single signaling conductor pair (or optical path), as contrasted to the parallel transmission of many bits in a byte or word of data as would occur among electronic components inside a microprocessor relay or a computer. Strictly speaking, Ethernet links among communicating devices are also serial, with only one wire pair or optical fiber in each direction, even though the data rates on these serial links are vastly higher than for RS-232 or RS-485.

Despite this fact, these two styles of communications are normally distinguished by calling RS-232 or RS-485 communications “serial”, as opposed to “Ethernet networks” or “Ethernet connections”.

Common Communications Devices:

1. Ethernet switch – provides a central connection point with orderly message packet handling for a number of computers and/or intelligent devices with Ethernet communications ports. Described briefly above and in more detail below.
2. Ethernet router – a computer that recognizes messages addressed to LAN devices, versus those addressed to some remote location. It isolates the local message exchanges from remote networks, and uses its address translation capabilities to send remotely-targeted messages on their way with cyber security protection of the messages and the LAN. Described in more detail in a section below.

Other Ethernet communications accessories such as hubs and bridges are either obsolete or not used in substation applications.

IEEE Device 16 in Substation Network Drawings

The proposal before the C37.2 Revision Working Group describes the use of Device Number 16 for a Data Communications Message Processing Device, handling protective relaying or other messaging traffic. Since there are many types of such devices, the following suffix list has been suggested to identify specific functions when a Device 16 box appears on a drawing:

- 16C – Security processing function (VPN, encryption, etc.)
- 16E – Ethernet component
- 16F – Firewall or incoming message filter function
- 16H – Hub (obsolescent)
- 16M – Network managed (SNMP) function
- 16R – Ethernet router
- 16S – Ethernet switch
- 16T – Telephone component

If the E suffix is not included, the box is presumed to be a serial networking device for RS-232 or 485 communications. These suffix letters can be combined to handle multifunctional networking devices as shown next. Figures 3 and 4 show examples of communicating electronic devices configured in substation protection, control, and data gathering applications.

Substation Integration with Serial Data Communications

Figure 3 shows what has been and remains the most widely used method of collecting data from microprocessor relays. The example has four multifunctional microprocessor-based relays, shown as Device 11:

- 11-1, a transmission line relay with directional comparison pilot line protection 85 based on distance elements 21P-1 and 21NP-1. The other device numbers show Zone 2 phase distance backup, directional ground overcurrent backup, and automatic reclosing.
- 11-2, a transmission line relay with 87L line current differential protection, 51 inverse time overcurrent backup, and 50BF breaker failure protection.

- 11-3, a transformer differential relay 87T with 51 phase and 51N neutral connection inverse time overcurrent backup, and 59 overvoltage protection.
- 11-4, a bus differential relay 87B with ground inverse-time overcurrent backup 51N.

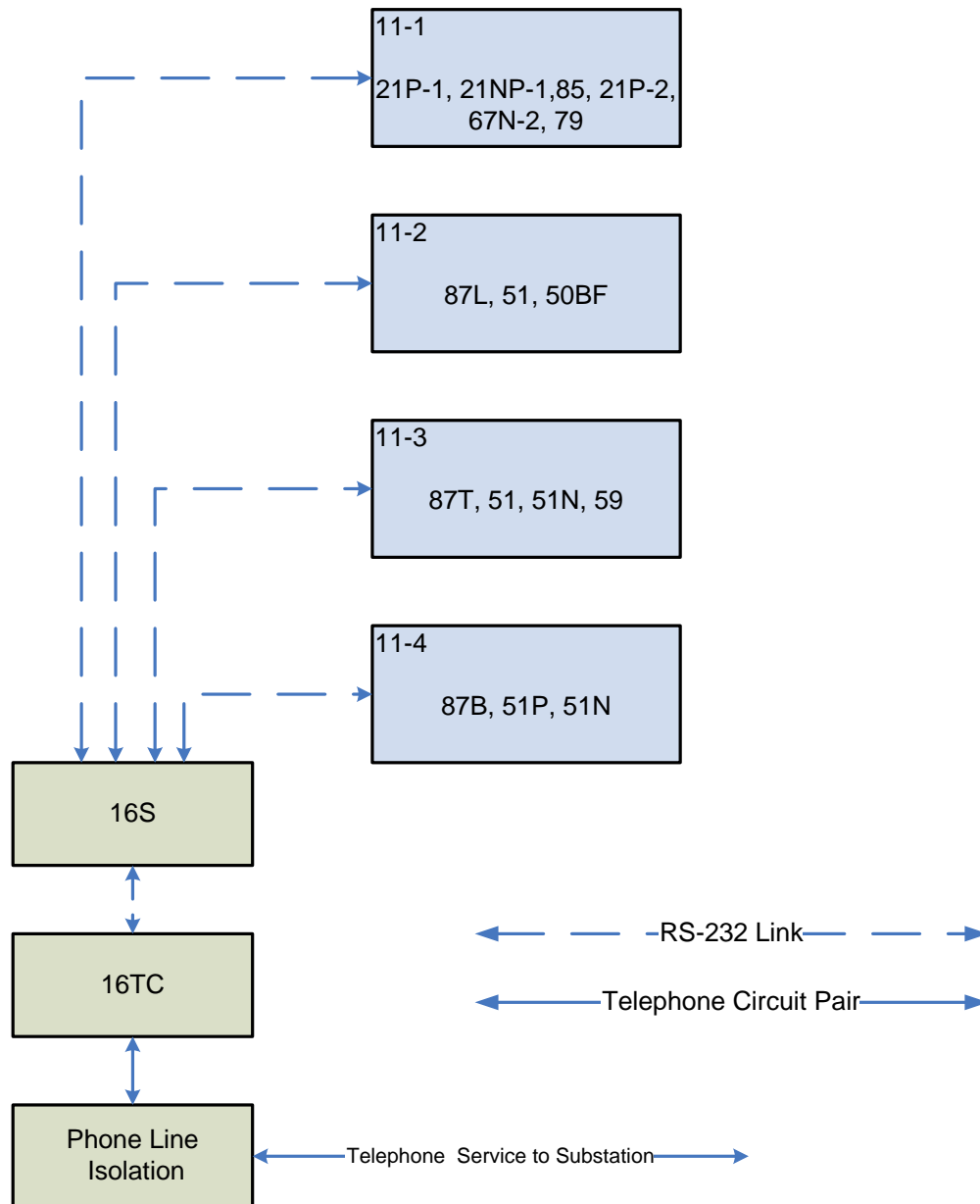


Figure 3 – Integration of RS-232 Communications with Devices of Type 16

Each of these relays has an RS-232 serial port. For integration of data communications, a substation might have the following:

- 16S - Each of the relay ports has a link connection to an RS-232 serial switch, Device 16S. 16S has a port through which a connected user can talk to the switch and request a connection to a particular end device – one of the four relays. The user can then upload status and metered values, fault location, event records, and oscillographic data as

available from the particular relay. The communications port is also used to download the large file of settings that is typical of modern relays. The device performing the 16S function may be a sophisticated communications processor with data storage, protocol translation, and information storage.

- 16TC – The switch or serial communications processor connects to the outside world through a modem – the familiar type would be device 16T. Typically, when 16T is used, the switch, communications processor, or each of the relays have a password for access security.

The designation 16TC indicates that this modem includes cyber security protection capability of securely encrypting the data communications messages. It can communicate only with a compatible modem at the other end of the communications circuit. Devices of type 16TC are becoming a popular solution to insure that substation devices cannot be accessed by unauthorized personnel, and to meet the requirements of NERC Critical Infrastructure Protection (CIP) standards that require combinations of physical and communications security against attacks on the power grid.

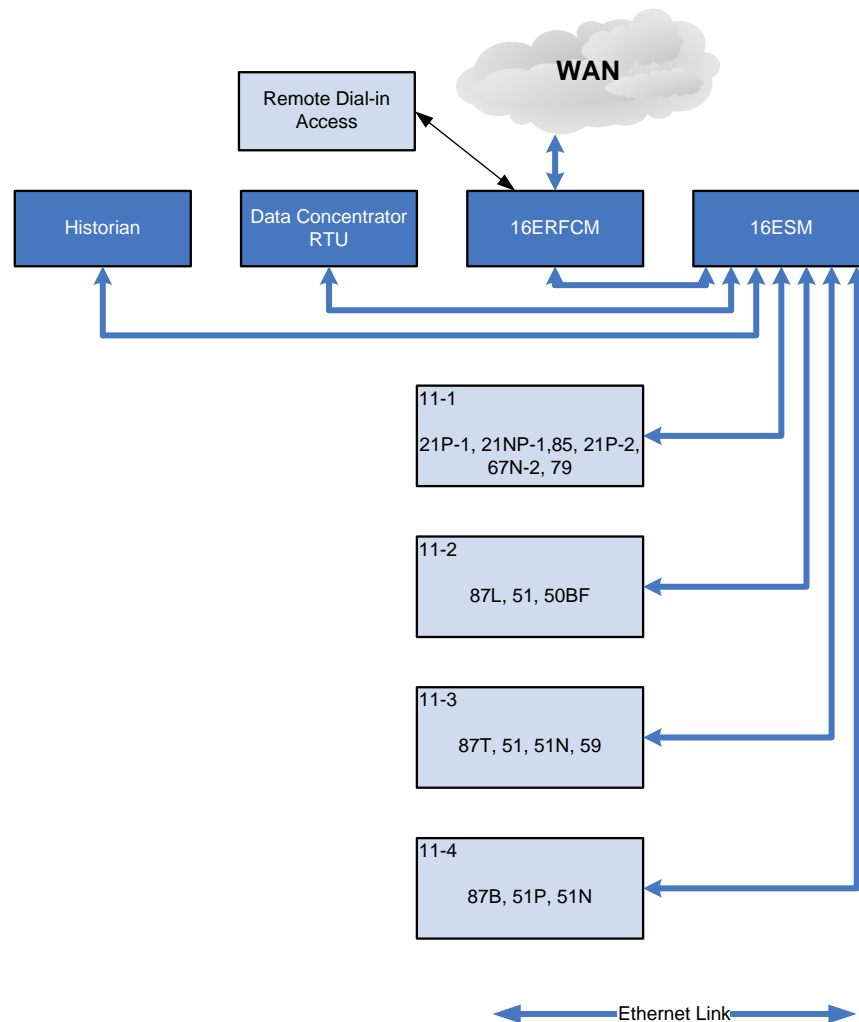


Figure 4 – Integration of Ethernet Communications with Devices of Type 16

Substation Integration with an Ethernet Network

Figure 4 shows an example of how the same group of relays might be integrated with an Ethernet LAN. It is possible to use the LAN to provide access to relays by dial-up telephone connection. However, the real benefit of using Ethernet is achieved when the network connection from the relays extends outside the substation to the utility enterprise shown as a wide-area network (WAN).

Each of the connections shown as one bidirectional arrow in Figure 3 comprises a pair of noise-immune optical fibers for conveying Ethernet message packets in each direction.

The new communications components in Figure 3 are:

- 16ESM – Ethernet Managed Switch. Each of the relay Ethernet network ports connects to a port on the Ethernet switch, described in more detail in a section below. The term “managed” refers to the fact that the switch operation itself can be monitored and controlled over the same network, and this is typically done from a remote location.
- 16ERFCM – Ethernet Router, managed, with firewall and VPN for cyber secured communications to the utility WAN. Routers are also described in a section below.
- Data concentrator/RTU – the substation-level central information processor. This processor polls all the relays and other IEDs via the Ethernet LAN for metered values, status, information records, and all other available data. It translates protocols as needed, and responds to control center polls and commands to replace the functionality of an RTU. It stores information in data bases that may be accessed later. Relay engineers, maintenance personnel, and managers can retrieve this data over the WAN using the office network tied to their computers. For a secure and backed up archive, the utility can upload the data and save it on a protected and backed up server in a remote office location. A maintenance person on the road can dial into the utility remote secure server, rather than directly accessing the substation.
- Historian - A separate PC runs a substation historian program in an important station. The historian continuously gathers states and values from the data concentrator and/or directly from relays and IEDs, acting like a trend recorder. Historian records can be used for asset condition monitoring or post-mortem events analysis. The substation historian may also communicate over the same network to the WAN, and on to a remote central enterprise historian, which gathers the records from all the substations and creates a single managed data base to serve utility asset managers.
- WAN – The substation LAN connects to an unspecified array of enterprise networks and work locations. The communications connection could be via utility-owned SONET (optical fiber ring data network), utility owned microwave system, or via common carrier data communications service. Two popular forms of the latter are Frame Relay protocol, or Multi-Protocol Layer Switching (MPLS) network, connected to the substation via an optical fiber or twisted metallic pair from a nearby service center of the communications provider.

Using Networks to Gather Operational and Non-Operational Data

Networked communications described in the last section make information from the substation broadly available to utility enterprise activities. Relay engineers, maintenance personnel, asset managers, and planners can all find information that helps them with their jobs. Records of fault operations, loading trends, files of settings, and oscillographic data records are referred to as *non-operational data*. Much of this information can be gathered by accessing particular relays or IEDs via dial up connections. However, as a practical matter, the time and effort required to gather and organize this data can overwhelm the staff, so the data is often collected only when there is a specific need, or a problem operation to analyze. With data concentrators and networked connection to the enterprise, this non-operational data collection can be automated so all the data is gathered, sorted, and made available to users who can benefit from it. These categories of users can create their own “back-office” (enterprise centralized) computer applications to parse all the data and extract useful information to help improve the utility management and business. For example, transformer loading profiles and temperature measurements can be gathered and automatically analyzed to predict loss of life, so that asset managers can forecast maintenance or replacement and budget the needed financial or human resources. Planners can use the same information to determine where system upgrades are justified. Overall, the financial benefits to the utility can make a good business case for installing the data communications systems and enterprise processing applications.

The LAN data collection and control message traffic through the relays to the Ethernet Switch and the data concentrator, for immediate use by SCADA operators, is described as *operational data*. Using relays and communications for system control operations brings a critically important benefit - using the data in this way inherently monitors to show that the relays are working correctly and measuring the power system voltages and currents as they should. This is achieved without a visit to the substation by test technicians. If the relay is observed to occasionally trip for a fault, we also know the breaker and its connections to the relay are verified. If no faults occur in the zone for a long time, the SCADA operator can trip and close the breaker remotely through relay communications at a convenient time to insure that protection is able to trip the breaker. As NERC institutes future maintenance requirements on critical protective relays, this *operational* integration and monitoring has the potential to eliminate the need for much of the field testing that would otherwise be required.

Ethernet Switches

The switch has the key role of tying together the bidirectional links from all of the LAN devices, and making the system work as a network in which any device can send a message to any other.

Figure 5 shows the basic functions of an Ethernet switch. A high-speed communications processor manages the flow of message packets among all the connected network links.

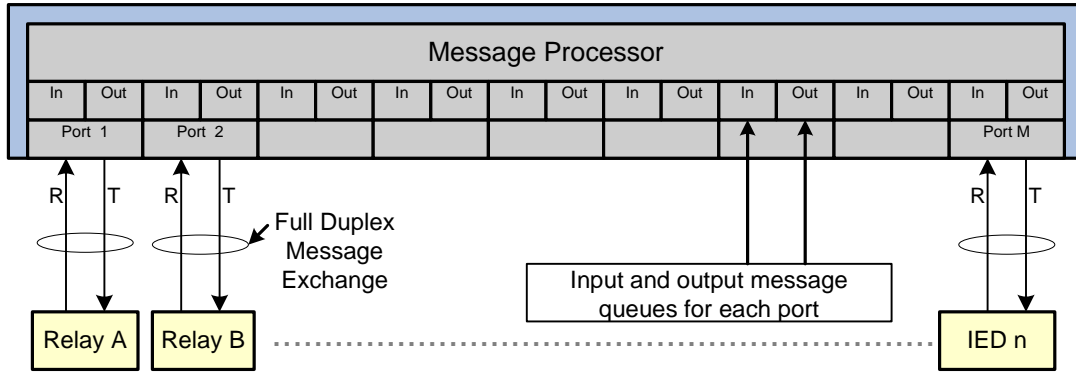
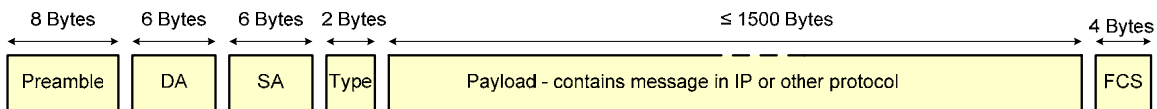


Figure 5 – Ethernet Switch

Physically, a typical switch is a 19-inch rack-mount unit that is 1 to 3 rack units high and has from 8 to 20 ports. Smaller units with 4 to 10 ports are made for panel or DIN rail mounting. Each connected link operates in full duplex mode – that is, messages can pass in either direction simultaneously and independently.



DA - Destination MAC (physical device) address
 SA - Source MAC (physical device) address
 FCS - Frame check sequence (error check)

Figure 6 – Basic Ethernet Message Packet or Frame Format

Focus on a particular incoming link, say from a relay transmitting an oscillographic file to be stored in the data concentrator. Figure 6 shows a typical Ethernet message packet passing through the switch. The parts of the message are:

- Preamble – sequence showing the start of the message for framing the rest.
- DA - the destination address - a media access controller address (MAC address), which is a unique number specifically assigned to the physical electronic hardware device that generated the message.
- SA - the source or sending device address, also a MAC address or physical device identifier.
- Type – identifier for special features in the frame.
- Payload – the desired data to be transferred. This includes higher protocol layers of level 3 and above. If the packet carries the Internet Protocol (IP) network layer 3, or other functionally related network layers, there is an IP address also buried here that is used to route the message. The switch deals only with layers 1 and 2, and does not pay attention to IP address.
- FCS – Frame check sequence - an error check calculated at the sending end from the frame bit sequence, and compared at the receiving end with a duplicate calculation there to detect if bits have been corrupted in transmission.

In its most basic operation, the switch takes each message in each incoming queue, checks it for errors, and places the message in all of the other outgoing queues. The switch goes from incoming queue to incoming queue looking for these messages and moving them. It does this processing in nanoseconds to microseconds per message – must faster than substation event resolution. It can handle even high rates of message input from many devices. The order of outgoing messages results from when the messages arrived and the order in which they were read, so the interleaving of the outgoing order can appear to be random. However, no messages are lost to mishandling or collisions. Lacking data corruption by noise or a hardware failure, the rapid arrival of the message at the other LAN devices is a certainty.

Each receiving IEDs checks each message to see if it is addressed to that device. This means that each link of the network carries a lot of unnecessary traffic that is intended for others and not used. Because each network link has such a high data rate capability of 10 to 1000 Megabits per second, this wasted message passing may not matter to the network. However, each of the IEDs has to look at each of the messages sent to it, and analyze each of the messages addressed to it. In heavy traffic, the processing ability of an IED may be taxed by a burst of messages.

Basic Switch Settings

Even in this simple operating mode, the switch has many settings that govern its behavior. For a typical example switch, the settings for each port can be:

1. Name of device or link.
2. Enable/disable port.
3. Type of communications medium (wire or fiber).
4. Speed.
5. Duplex mode – half or full.
6. Enable/disable auto-negotiation with the connected device of speed and duplex mode
7. Enable/disable flow control – output port sends pause messages back to source ports that are sending too much data, to regulate flow of packets.
8. Enable/disable link failure indication (LFI) to the connected device.
9. Link alarms on/off.
10. Ingress limit – the maximum frame rate that will be accepted before excess incoming data is discarded.
11. Types of incoming messages to limit and discard (all types including addressed messages, broadcast messages without destination address, multicast messages without destination address including IEC 61850 GOOSE relaying messages).
12. Egress limit – the maximum frame rate to be transmitted to the connected device. Excess message packets are discarded by the switch.
13. Port mirroring enabling and selection – when enabled, the port carries the same output data as another chosen port, for diagnostic use.
14. Power-over-Ethernet settings – an additional list of settings for powering devices over wired link connections with set voltage and current limits, if enabled.

Each switch may have from 4 to 20 or more ports, each with such a setting list. This list does not show additional settings for advanced features discussed just below. It is possible to have over 1000 settings based just on the parameters listed above, although only a fraction of these are actually changed from default values in a typical application. Keep in mind that an unused but incorrectly set feature can still cause operating incompatibilities.

Additional Capabilities Used in Substations

Figure 7 shows an Ethernet frame with added information that enables features defined in newer subparts of the Ethernet standards set.

Virtual LAN

The VLAN ID tag permits the sending device to specify the message as belonging only on one out of a number of virtual subnetworks that all coexist on the one physical LAN. Each VLAN comprises a number of devices that are designated to receive messages identified for that VLAN; these VLAN tagged messages are not sent to other devices not on that particular VLAN. See Figure 8, where high-volume critical messages such as IEC 61850 GOOSE messages (see below) are assigned to VLAN 1 so that the substation control and monitoring IEDs on VLAN 2 will not see them.

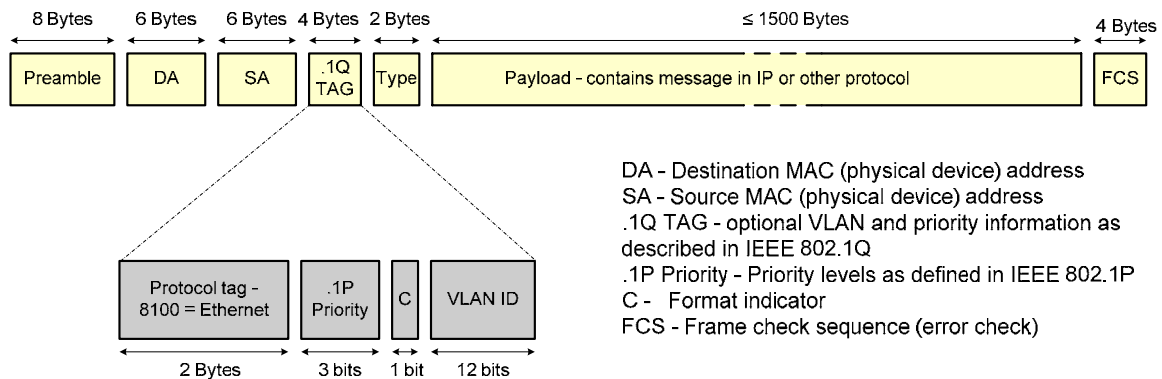


Figure 7 – Ethernet Frame with VLAN & Priority Tag

Switch configuration settings define the VLANs that exist on the physical LAN. VLANs can be defined either by assigning specific ports to a desired VLAN, or the VLAN can be defined by a list of MAC addresses. If a message has a VLAN tag, it is passed only to the ports or to the MAC addresses assigned to that VLAN. Using port assignments makes replacement maintenance easier in a substation.

While over 4,000 VLANs can be defined, a typical substation only needs a few. In our example switch, there is a setting to make the switch VLAN aware, so that every port is on some VLAN. Each VLAN the user configures is set to assign a number and 3 other settings. Each port can have 4 VLAN association and behavior settings. MAC address based VLANs are defined in tables that also are settings.

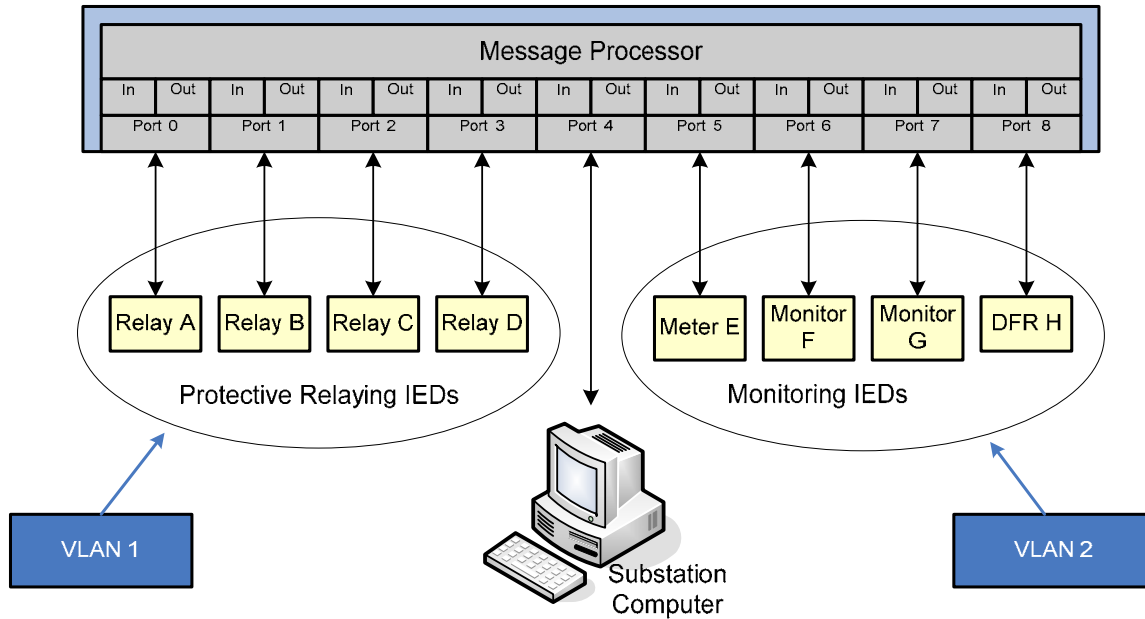


Figure 8 – Substation Ethernet Devices Segregated Using Virtual LANs (VLANs)

Message Priority

With the enhanced frame of Figure 7, a message can be assigned a priority of zero to 7. The switch reads the priority value, if the tag is present, and reorders messages in the queue according to priority. See Figure 9. The most important messages are pushed to the outgoing end of the queue so that they are sent right away. In this way, a critical fault-tripping GOOSE message would not be delayed waiting in line behind transmission of a large packet containing oscillographic data from some prior fault to a remote engineering server.

Priority in message handling can also be implemented by recognizing the specific hardware unit that is sending or receiving the message (MAC address), or by reading class-of-service (CoS) information in messages using the internet protocol. An example switch might have 3 settings for overall enabling and behavior of priority handling, plus six settings for each configured port – up to about 100 settings.

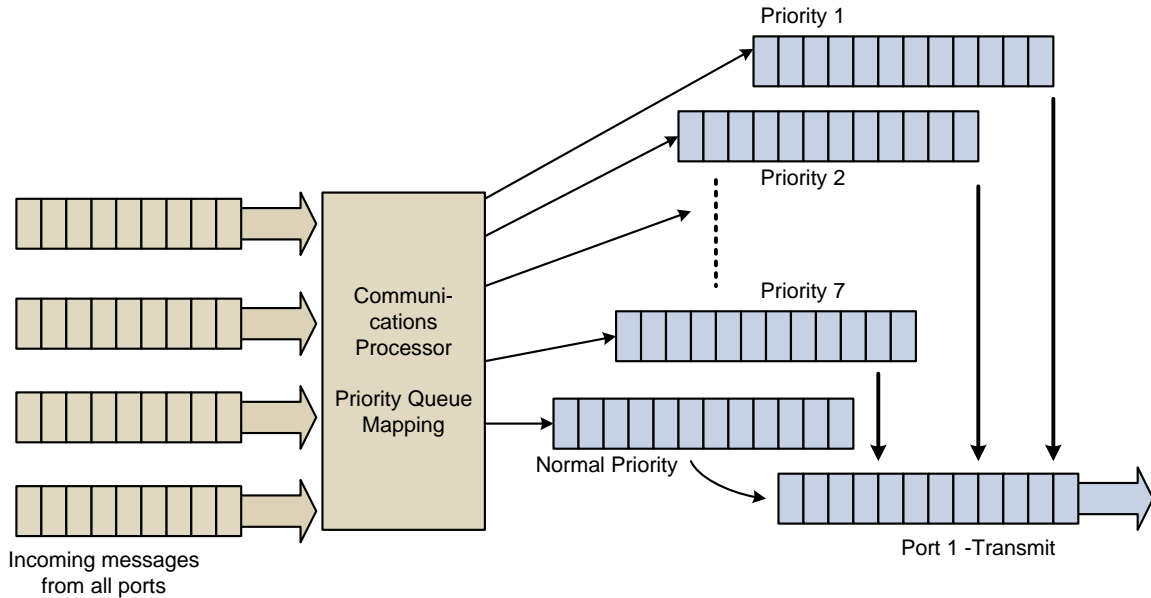


Figure 9 – Priority Bits Used to Order Messages in Queue

Rapid Spanning Tree Protocol (RSTP)

The switch has the capability to discover or learn about redundant paths in a physical network configuration. For example, this can arise if multiple switches are connected in a ring to provide the redundancy of multiple physical paths in case one path should fail. This is one of multiple techniques that can be used to insure network redundancy for reliable relaying applications.

With RSTP enabled, certain switches will learn to block message transmission through selected ports in order to break a loop – to keep a single message from circulating around the ring indefinitely. If some message path fails, the switches discover the failure, and automatically re-enable the previously turned-off port to restore service to the failed loop section from the other direction.

For a typical example 20-port switch, RSTP capability adds 8 more overall settings, plus 7 settings per switch port, for a total of 148 more configuration settings.

Multicast Message Filtering

For multicast messages without specific destination addresses (including GOOSE messages used for relaying), the switch can be configured with fixed multicast groupings of ports, so that not all multicast messages are passed to all ports.

Static multicast grouping looks for a multicast message from a particular physical device (identified by MAC address) and assigns it only to a specific VLAN; the other VLANs will not see this message. Dynamic grouping is also supported, although this is not typically used for a substation LAN. With the Internet Group Management Protocol (IGMP) enabled, the switch can receive commands or detect indications that certain groupings have been turned on or off, and can dynamically adjust its routing of multicast messages to certain VLANs or ports according to specified settings.

Multicast message filtering adds at least 5 settings plus 4 more static grouping settings per VLAN if used. While this may appear to be a small number of settings, the interactions of switches, routers, VLANs, and messages is full of application subtleties and behavior cases that are taught by switch manufacturers in their literature and instruction courses. Defining these settings can take careful planning.

Switch Management Information

Switches are managed by computers tied to them via the LAN or WAN, or sometimes via a serial port on the switch. The standard messaging protocol for configuring management access is simple network management protocol (SNMP). A switch may be configured for:

- Identification
- Passwords
- Time and date
- Levels and groups of users and access security for each
- Addresses
- Handling of internet protocol (IP) messages
- Routing of switch event or trouble messages
- Reporting of operating statistics
- Events and alarming of problems (e.g. number of packets with errors at a particular port)

Each event or alarm is configured by the user with from 6 to 10 settings. So setting up switch management can easily require hundreds of settings.

Switch Setting Summary

Depending on the features selected or needed by the user, a typical substation switch will have from several hundred to over 2000 settings. Even though many of these features are not to be used, incorrect enabling of features can cause operating problems on the LAN.

Users of modern multifunctional microprocessor relays are now accustomed to relays that have over 1000 settings defining core behavior and logic as well as reach values and pickups. One wrong setting can cause a false trip. The industry is becoming aware that relay setting records need to be centrally archived, and periodically checked between the archive and the relays in the field. The setting records must be protected via a tight management system to avoid relay misoperations due to setting errors. For deeper discussion on this current protection issue, see [2], presented in conjunction with the present conference.

Reviewing the features of Ethernet switches and the number of settings that affect behavior, it becomes apparent that systems for relay settings management may be needed for the Ethernet switch setting records as well. Since switches are increasingly carrying critical protection and SCADA control traffic, the liabilities for setting control problems are becoming similar to those for the connected relays.

At the IEEE Power System Relaying Committee and at the Substations Committee, working groups are beginning to look at developing industry guidance for dealing with settings of switches and routers.

Ethernet Routers

An Ethernet router serves as an interface between a local area network in a substation and the utility enterprise WAN. Since the WAN comprises far-flung segments accessed through long-distance data communications, which may be utility-owned or common carrier (purchased service from a communications company). To communicate with other parts of the WAN, the router must handle message reformatting to utilize the available data communications path. It may also need to provide cyber security protection so that messages sent across unprotected networks cannot be monitored, disturbed, or corrupted by unknown persons.

Physically, the router is another communications computer like a switch, typically in a 19 inch rack mount package of 1 to 3 rack units. It has fewer ports, since its role is to interface one or two LANs with one or a couple of external communications circuits. While switches tested to IEEE 1613 environmental standards (see the next section) have been available for years, IEEE 1613 routers have become available recently.

The router processor handles a larger array of functions, algorithms than a switch. It carries out sophisticated manipulation of layer 3 (network layer) routing information in the message payload, which switches generally ignore. It may also manipulate the contents of the message packet as shown above and defined in layer 2. There are potentially thousands of user settings, defining a database that describes how the WAN and the networked world outside the substation are accessed. This is required so that the router can direct messages through the WAN or even the Internet to remote resources requested by devices or users in the substation; and can recognize the origin of incoming messages.

The functions in an example router include:

1. Ability to learn about remote servers on the WAN, including those that provide translation of domain names to numerical internet protocol addresses. Alternatively, static WAN configuration data can be manually entered.
2. Ability to translate addresses on the LAN to different addresses on the WAN or Internet for proper routing and for cyber security protection of LAN devices.
3. Firewall to protect substation LAN traffic and devices from unauthorized access.
4. Virtual Private Networking (VPN) using any of several standard protocols – establishing an isolated communications tunnel through an insecure public communications network to a secure remote utility server, with strong encryption of messages that protects against disruption or monitoring of message flow.
5. Recognition of external communications traffic from the LAN; routing and prioritization of this external message traffic in both directions.
6. Routing of multicast messages to LANs or VLANs at remote sites (generic routing encapsulation, GRE). Recall that multicast messages do not have destination addresses, and must be recognized from their sources.
7. Ability to assign and manage IP addresses of devices on the LAN that request them (although in substations the IP addresses of relays and IEDs are usually fixed as settings in those units) (dynamic host control protocol, DHCP).
8. Recognition of external path failures and rerouting of traffic via alternate paths (virtual router redundancy protocol, VRRP).
9. Reformatting of messages for compatibility with a variety of external communications channel types, for example:
 - a. T1/E1 (e.g. utility owned fiber ring or microwave)
 - b. T3/E3/DS3 (e.g. utility owned SONET)
 - c. Frame Relay (common carrier)

- d. Multi-protocol layer switching (MPLS) (common carrier)
 - e. Ethernet connection to WAN
 - f. DSL to common carrier
 - g. Serial RS-232 and RS-485 (e.g. to old SCADA master)
 - h. Modem over telephone circuit or voice channel
10. Monitoring, alarming, and logging of traffic behavior and diagnostics.
 11. Network management protocol (SNMP) communications for router and network management.
 12. Secure shell (SSH) network web server communications with a remote management computer/server.
 13. Receiving and serving date/time information to the LAN (network time protocol, NTP; and simple NTP or Sntp).
 14. Facilities for backing up and restoring the full configuration or setting data base.

On this last point – as we discussed for switches, the saved data base should be handled and managed like settings of an important relay. Many of the settings and values impact the coordination of the router performance with remote routers and computers on the utility network, and network communications may fail if the data base restoration is not accurate and precise. It is critical to have a setting archive and a setting restoration work plan if the router fails and is replaced in the field, just as for a complex relay.

Environmental Hardening – IEEE 1613

Ethernet switches and routers will be subjected to the same substation electrical and physical environment as the relays connected to them. Accordingly, they should be able to pass environmental tests simulating the substation environment. IEEE Standard 1613-2003 [3] lists the required tests for a substation-hardened data communications device, using testing methods parallel to those in relay electrical and physical environmental test standards from IEEE. Switches and routers designed for office or data center IT applications generally cannot pass IEEE 1613 – the robustness needed must be designed into the device and verified during development.

IEEE 1613 sets requirements for:

1. Operating temperature – at least from -20 to +55 degrees C, with wider ranges up to -40 to +85 degrees C.
2. No cooling fans can be used to meet temperature specifications.
3. Operation at prolonged high humidity.
4. Dc supply voltages and ripple from station battery (ac is an alternate).
5. Dielectric tests for insulation barriers of low-voltage communications circuits, and for circuits connected to higher voltages such as control power inputs or alarm contacts.
6. Impulse voltage tests of 5 kV for insulation barriers of circuits other than low-voltage circuits.
7. Oscillatory SWC test, 2.5 kV 1 MHz decaying wave.
8. Fast transient SWC test, 4 kV for 50 ns.
9. RFI susceptibility test, 35 V/m from 80 MHz to 1 GHz.
10. Electrostatic discharge (ESD) tests as in relay standard C37.90.3.
11. Vibration and physical shock tests as in IEEE C37.1.

IEEE 1613 defines two classes of conformance for each category of influence immunity:

- Class 1 – may have temporary data errors during disturbing influences, but no damage.

- Class 2 – continues to handle data correctly during the particular types of influence tested.

If relaying or time critical operating data messages pass through the communications device, class 2 capability is required.

IEEE 1613 compliant devices should be used for substation applications whenever a device with suitable functions is available. Occasionally, an application could require a device with a functional capability not available from any 1613-compliant device. This has most often been true for routers used to connect a common-carrier network, although 1613-compliant routers with capabilities needed for large scale IT enterprise integration are now available. Installing a generic router requires:

- Providing a surge-immune inverter to power the device having an ac power supply from the uninterruptible dc battery supply.
- Controlling electrical surges and interference to the power supply.
- Using optical fiber or optically isolated data connections to minimize surges on communications circuits.
- Controlling the temperature and physical environment with heaters, air conditioning, and air filters.
- Checking on condition of cooling fans during substation visits.
- Setting up an action plan for device failure, or having a backup access to the substation network.

IEC 61850 GOOSE Messaging

When switches and routers convey GOOSE messages, they perform critical protective relaying functions, and thus become as important as any other auxiliary relays to power system security.

GOOSE Messaging Operation

Most of the information or control messages in IEC 61850, DNP3, or other protocols that can operate on an Ethernet LAN are single transmissions of snapshot values or requests. By contrast, IEC 61850 GOOSE messages are designed to convey an effectively continuous indication of the state of some logic or control point, or analog value, so that the messages can replace control wiring. GSSE messages defined in IEC 61850 perform the same function, but only for binary states, using the approach of the forbear EPRI UCA™ LAN protocol.

Publisher-Subscriber Model

The GOOSE message is not addressed by the sender to a particular receiving relay. Rather, it is sent as a multicast message that goes onto the LAN with identification of who the sender is, so that its control information contents can be determined by any listening relays or IEDs that require it. Every other relay and IED on the LAN or VLAN can hear the message, and decide on its own whether it needs to look at the contents from the particular sending relay (based on source address value as compared to listener settings).

The transmitting IED is called the publisher, and any other relay or IED that is configured by settings 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. In early implementations by vendors of GOOSE

messaging, the message publication and subscription is set up manually by the user (with relay settings). However, the messages on the LAN are genuine GOOSE messages that are fully compliant with IEC 61850 specifications. This means that relays from multiple vendors can all subscribe to and properly interpret a GOOSE message from any manufacturer’s publishing relay.

GOOSE messaging is an unconfirmed service. This means that the publisher has no way of finding out if all the subscribers got the latest information – in fact, it does not even know who all the subscribers are. 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. Thus each publisher sends its state or value messages over and over again, 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 10 illustrates the message repeat interval variation. 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 millisecond values, adequate to keep the subscribers updated on the latest state for relaying purposes as the power system event evolves. After the power system stabilizes again, the GOOSE message logic in the publishing relay notices that states are not changing any more, and backs down to a lower stable state rate of message transmission, as shown in Figure 10. 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.

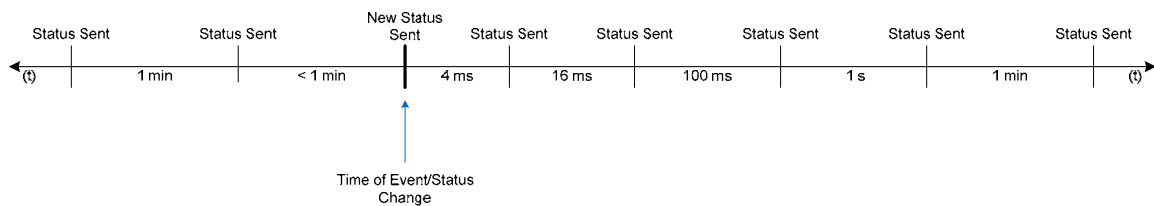


Figure 10 – Adaptive Timing of GOOSE Message Transmissions

The continuous low rate GOOSE message transmission allows any new or replaced subscribing relay to be updated on critical states it needs, since it cannot ask for a transmission. What is particularly valuable is that all the subscribing relays can be set to alarm if the periodic updates are not received on time. This yields remote alarms for a failure of the publisher, of any network component between the publisher and subscriber, and of the subscriber network data interface. Monitored network components include fiber connections and Ethernet switches. Conventional wiring is not generally capable of this non-invasive continuous monitoring process – it must be periodically tested. Thus, network-based relaying can help to cut utility maintenance costs.

When a fault occurs, a relay must be able to recognize, decode, and act on subscribed messages fast enough to meet protective relaying requirements. In general, the application-to-application messaging time should be less than 4 ms. In practice, GOOSE messages have been shown to

convey operating commands as fast as or faster than wires carrying contact signals from one relay to another.

GOOSE Messaging Applications

In new substation designs, GOOSE messaging is used to replace wiring and panel switches for critical protection. Functions for which GOOSE messaging can be used 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.

Network Redundancy

In transmission substations, protection schemes use two sets of protective relays for each zone. Thus full high-speed protection continues if one system fails or is removed from service for maintenance. The two redundant systems are almost completely isolated. This is in addition to remote backup zones that provide additional fault protection with more time delay.

When some of the fault protection measurements or control signals are exchanged over the LAN, the LAN architecture needs to have redundancy as well. The most straightforward approach is to connect all the relays in redundant relay set A to one switch or grouping of switches, and to separately connect all the relays in set B to a separate switch or grouping of switches. This meets the basic criterion that a single LAN failure will not take out both redundant systems protecting any substation zone.

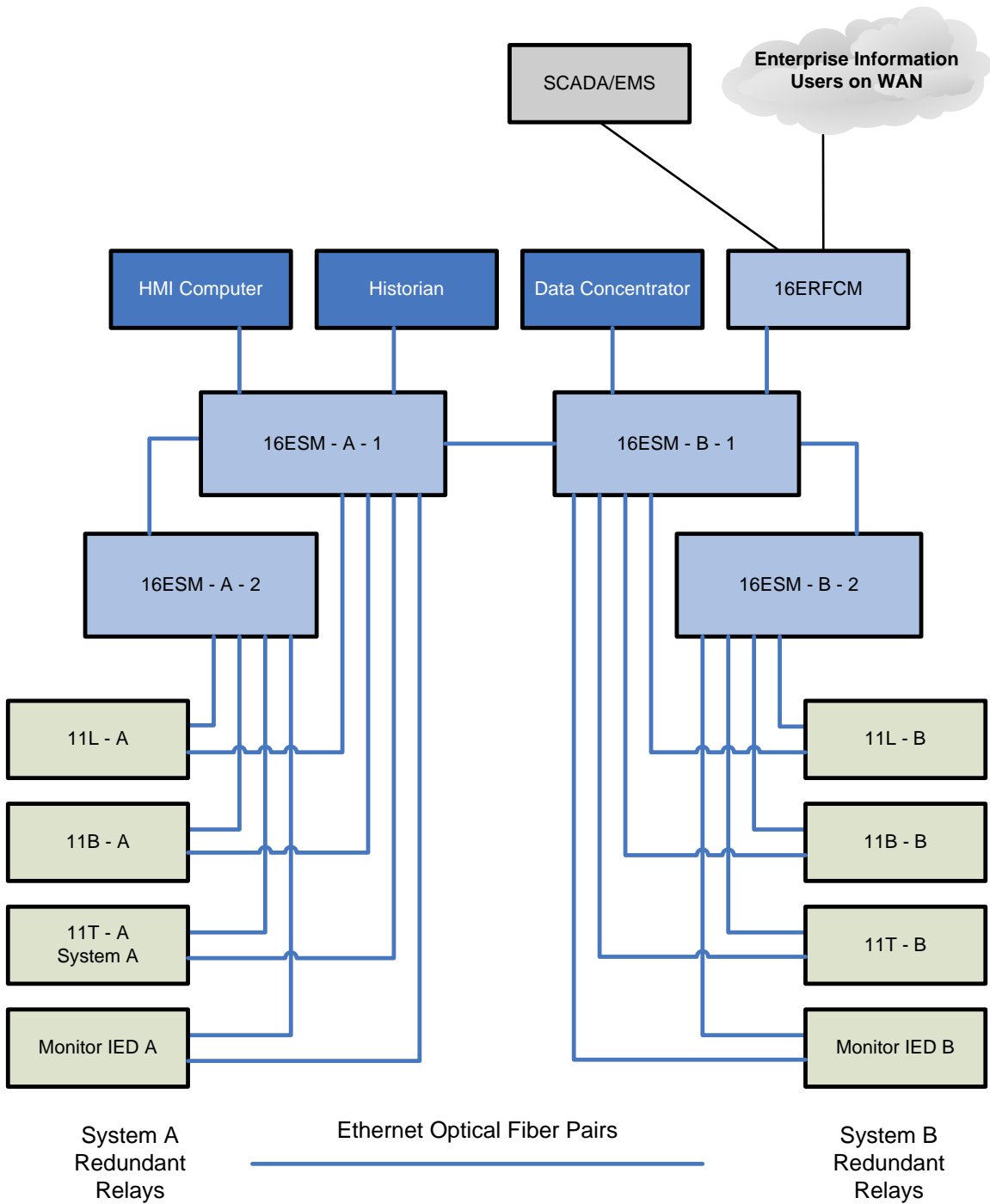


Figure 11 – Redundant LANs Having Primary and Failover Links in Each LAN

However, a failure in the LAN of redundant Set A may impact more than one zone of protection within the redundant Set A. To limit the failure effect to a single zone at worst, LAN designs may include redundancy *within* the Set A or Set B networks so that a single LAN failure has no functional impact or impacts one relay at worst. The strategies for doing this are:

1. Connect multiple switches in a ring, so that there are at least two paths from any switch port used by a relay to any other such switch port. In the discussion of Ethernet switches above, we described rapid spanning tree protocol (RTSP) by which the switches would learn and use a normal or default message path without circulating messages forever in a loop. If the ring breaks, the switches can detect the failure and set up new routing of messages to maintain communications.
2. Many GOOSE-capable relays have primary and failover communications ports. Provide two switches or switch groups within the redundant Set A (and also in Set B). Connect the primary port to one switch or switch group, and connect the backup port to the other switch group. See Figure 11. The net result is that there are always two or more paths from any relay to any other within the redundant set.

The switch groups are also cross-connected so that substation level IEDs – the data concentrator, HMI, historian, WAN connection from router, and others - can access relays in both redundant sets. Also, GOOSE messages can pass between redundant sets. The switch port traffic management features provide suitable isolation of the redundant LANs.

IEC 61850 Process Bus Messaging

Figure 12 shows how the Process Bus part 9-2 of IEC 61850 might be used to transmit streaming raw sampled data values from the switchyard over optical fibers to relays in the control house. A few optical fibers arranged in a LAN carrying 61850 message traffic can replace a mass of wires from conventional instrument transformers into the control house where they connect to relays and other measuring IEDs.

Process bus LAN applications will further raise the criticality of switch settings and application. Relays will depend on Ethernet switch and LAN configuration and performance to perform their basic protective measurement functions. Protection engineering will necessarily include knowledge and understanding of switch and LAN characteristics.

GOOSE messaging has been successfully applied for commercial use in many substations, but process bus applications to replace conventional switchyard wiring and connections are less developed and still emerging. The few installations in service are experimental.

Figure 12 does not show redundancy in the LAN design for switchyard data acquisition and control, but obviously a good redundancy design as discussed in the last section is essential. In this case, the data stream from one electronic voltage or current transducer must serve more than one zone of protection, so the design must keep a single LAN failure from impacting multiple zones. The architectures for this are still being evolved. For deeper discussion, see [4].

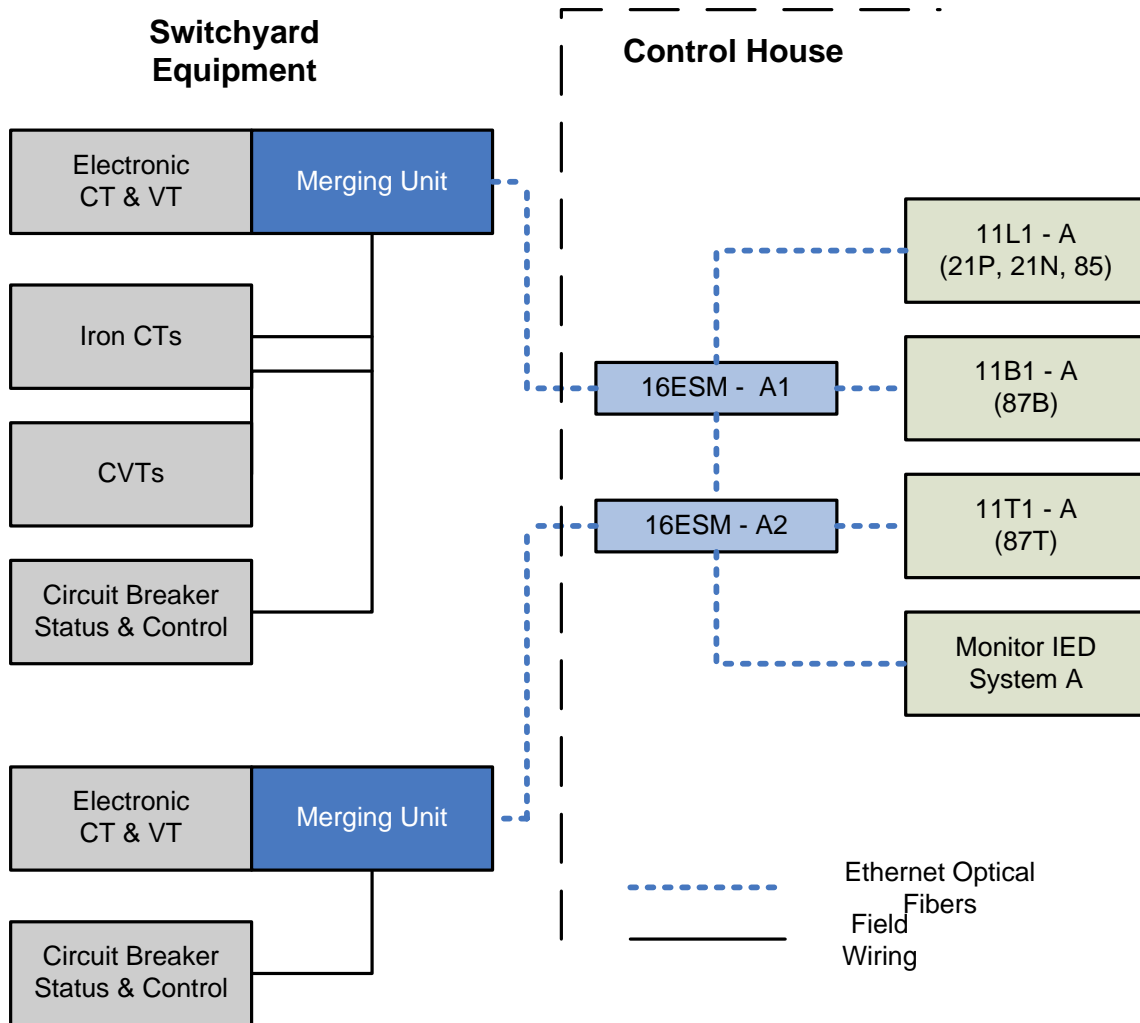


Figure 12 – Ethernet Switches in IEC 61850-9-2 Process Bus Application

Who is responsible for switches, routers, and settings?

The entire development of this paper leads to the conclusion that protection and control engineers must take responsibility for application of LANs and communications devices like Ethernet switches that carry out basic functions of the system. The LAN technology is complex to use and requires the same education and attention as for the rest of the protection and control scheme. However, adequate understanding and proper application are well within the reach of relay engineers dealing with modern microprocessor relays and substation control systems.

Most protection and control engineers don't have a deep understanding of how to configure and apply LANs or the communications appliances that make them work. Switches and routers are as complex to apply as relays – we have pointed out the long lists of settings, and the application subtleties on which individual IT experts build careers.

If it is a challenge for relay engineers to understand the subtleties of networking, it is similarly a challenge for IT experts to understand the requirements for system protection or the consequences

of errors. The deep evaluation of single points of failure, the ability to conduct maintenance with no allowance for even a short outage of a critical function, the risks of false tripping from corrupted or missing data, and the need to analyze and explain in full technical detail misoperations so that remedies can be documented and applied – may all be approached quite differently in the system protection and IT worlds.

This situation brings the risk for organizational conflict. The operation of switches and routers, and the architecting of LANs and WANs, has been in the domain of IT departments for decades before they became relevant to relaying and control. Because of this, the IT departments at many utilities specify products to use, connect up the LANs and WANs, and manage the settings and configuration. Protection and IT departments can become polarized over who controls the substation LAN. The situation is somewhat like the conflict that arose between relay and SCADA engineers at some utilities decades ago.

As with integration of SCADA and protection, the only forward-looking solution for substation control and protection LANs is interactive cooperation of protection and IT teams. Each of the parties has half of the knowledge required for successful implementations that meet the needs of substation protection and control along with enterprise IT users.

The author contends that the utility industry needs an education and cooperation initiative that bridges the gap, before continuing widespread deployment of substation LAN projects. Utilities, vendors, and universities have an opportunity today to team up to create programs for cross-training of IT and protection-control engineers and technicians, as well as managers. Cross-trained teams will avoid operating and management problems that might otherwise occur, and are also likely to invent new approaches and applications that take advantage of technology advances in both fields. IT technology is sold to a large worldwide market, and is moving especially quickly.

Conclusion

The paper has used the proposed creation of IEEE Device Number 16 as a launching point for a tutorial overview of communications equipment and networks in modern substation protection and control systems. Examples for use of various devices of Type 16 are given. These LAN components and architectures are critical to control and protection in new substation designs, but have received little attention from the relaying community so far. By describing some applications and settings, this paper has characterized Ethernet communications devices as approaching the importance and complexity of the relays with which they work. Application and configuration has subtleties that are understood through study and experience - protection and control engineers would find the process to be familiar.

The IEEE Power Engineering Society – Substations Committee, and the Power System Relaying Committee, are establishing a task force to determine what sort of standards project would be helpful to the relaying and control community as it begins to use Ethernet switches and routers.

Beyond this, the paper proposes an initiative among utilities, manufacturers, and universities for cross training to help avoid the creation of organizational walls between IT and protection/control groups that must work together for successful future substation integration projects.

The Chairman of the IEEE Substations Committee – Power System Relaying Committee Joint C37.2 Revision Working Group is John Tengdin, j.t.tengdin@ieee.org.

References

1. IEEE C37.2-1996 (Reaffirmed 2001) – *IEEE Standard Electrical Power System Device Function Numbers and Contact Designations*.
2. IEEE Power System Relaying Committee, Working Group C3, *Processes, Issues, Trends and Quality Control of Relay Settings*, Final Version 7.3, March 2007.
<http://www.pes-psrc.org/c/>.
3. IEEE Standard 1613-2003, *IEEE Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations*.
4. Kasztenny, Whatley, Udren, Burger, Finney, and Adamiak, *IEC 61850: A Practical Application Primer for Protection Engineers*, Georgia Tech Protective Relay Conference, 2006.
5. Skendzic, V. and Moore, R., *Extending the Substation LAN Beyond Substation Boundaries: Current Capabilities and Potential New Protection Applications of Wide-Area Ethernet*, Western Protective Relay Conference, 2006, or available at <http://www.selinc.com/techpprs.htm>.
6. Pozzuoli, R., *Ethernet in Substation Automation Applications – Issues and Requirements*, available at <http://www.ruggedcom.com/whitepapers.html>.



Eric A. Udren has a 37 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. In 1969 he joined the Westinghouse Relay-Instrument Division, where 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 1990, he transitioned from Westinghouse to the ABB Protection and Automation Division. He led the design of the first interface of a microprocessor protective relay to an optical current sensor for installation at TVA. In 1996, he joined Eaton Electrical (Cutler-Hammer) in Pittsburgh, where he served as Engineering Manager for Electronic Products. In 2004, Mr. Udren joined KEMA T&D Consulting in Raleigh, NC as Senior Principal Consultant. 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. He also contributed to strategy and technical design for utility enterprise integration of information from substations.

Mr. Udren is a Fellow of IEEE, Member of the IEEE Power System Relaying Committee (PSRC), and Chairman of two PSRC Standards Working Groups. On two occasions, in 2001 and 2006, he received the PSRC Distinguished Service Award. 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. Eric now serves on the NERC System Protection and Control Task Force, leading development of protection and control maintenance approaches. He has written and presented over 40 technical papers and chapters of books on relaying topics, and has taught courses on protection, control, communications, and integration. He holds 8 patents on relaying and power-system communications.