Selecting, Designing, and Installing Modern Data Networks in Electrical Substations

Gary W. Scheer and David J. Dolezilek
Schweitzer Engineering Laboratories, Inc.

Presented at the
International Conference & Exhibition:
Relay Protection and Substation Automation of Modern EHV Power Systems
Cheboksary, Russia
September 9–13, 2007

Previous revised edition released May 2007

Originally presented at the
9th Annual Western Power Delivery Automation Conference, April 2007

Selecting, Designing, and Installing Modern Data Networks in Electrical Substations

Gary W. Scheer and David J. Dolezilek, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Equipment, software, and standards have advanced over the last seven years as suppliers, consultants, integrators, and electric utilities have gained experience using data networks in electric substations. Functionally, these networks provide operational (SCADA) data, engineering and analysis access, and high-speed interdevice data exchange. This paper identifies the major functions of these networks and their components. We examine and compare serial and Ethernet architectures for an example substation using the following criteria:**

- **Reliability**
- **Cost of equipment and commissioning**
- **Safety**
- **Ease and cost to design, implement, maintain, and expand**
- **Effective data transfer rates**
- **Performance of high-speed control signals**

The paper describes the methods to analyze networks for different applications, while providing a qualitative and quantitative comparison for the example station.

I. Introduction

Electric utility engineers have discussed Ethernet networks in recent years and installed pilot or demonstration systems to evaluate their application for protection, monitoring, automation, and control. These early Ethernet systems provided needed insight into the state of the art; however, they did not consider the traditional acceptance criteria of cost, reliability, performance, and ongoing maintenance.

IEC 60870-4, Telecontrol Equipment and Systems Part 4: Performance Requirements [1] is an international standard that applies to telecontrol equipment and digital communications. Since its publication, telecontrol and substation automation systems have migrated toward less centralized designs of networked intelligent electronic devices (IEDs). However, the object of the standard excerpted below and the methods and tools expressed within it remain applicable today, and they are especially useful when comparing Ethernet to other communications designs.

"This part [of IEC 60870] deals with those characteristics which affect the performance of telecontrol systems and relates the characteristics to the application and processing functions.

The object of this part is to establish a set of rules, which can be used to assess and specify the performance requirements of telecontrol systems.

This paper uses many of the international standardized methods of performance comparison for substation equipment presented in [1] as well as other well-known industry references.

Ethernet networks provide benefits and shortcomings compared to other approaches. It is essential to identify and measure these trade-offs to make credible, logical comparisons and decisions based on data. These trade-offs drive the selection of system features and benefits, the measures of success, and define areas for improvement. This paper compares several contemporary integrated communications topologies available to meet the instrumentation and control (I&C) demands of a typical substation. Multiple architectures are contrasted, including popular serial and Ethernet substation local area network (LAN) designs that support the most widely used IED protocols. In order to satisfy demands in the substation, as well as remote users and processors, systems include one or more devices acting as information processors. Information processors are required to provide some or all of the following features, depending on the specific system applications.

1. Act as an upstream gateway to connect to SCADA and other enterprise applications.
2. Perform channel diagnostics and visualize parameters for troubleshooting.
3. Support multimedia connections of copper, fiber, and wireless serial and Ethernet connections.
4. Perform protocol conversion between various different clients, servers, information processors, and IEDs.
5. Concentrate data extracted from IEDs to filter out unnecessary data and to combine data from multiple IEDs into data sets.
6. Support interleaved conversations so that eight or more necessary conversations don't require eight or more physical connections.
7. Segregate IEDs so that they receive and process only the information destined for them, thus freeing the IEDs from unnecessary communications processing.
8. Prioritize important protection and automation messages to assure rapid, deterministic delivery.
9. Store and forward all received message traffic to eliminate message collisions and assure consistent delivery of data.

This paper compares serial systems, in which all nine features are built into one information processor, with Ethernet systems, which use two or more devices acting together to serve as the information processor.

The paper also addresses connecting these systems to legacy remote SCADA connections and local operator interfaces. These architectures are compared using the following criteria:

- Reliability
- Cost of equipment and commissioning

- Safety
- Ease and cost to build communications networks and physically connect devices
- Ease and cost to create configuration of devices and network components
- Effective data transfer rates
- Performance of high-speed control signals
- Ease and cost of maintenance
- Ease and cost of expansion

We examine these alternatives for a substation with two line connections, two transformers, and four feeders.

The reliability analysis draws on our earlier paper, "Comparing the Reliability of Ethernet Network Topologies in Substation Control and Monitoring Networks" [2]. Since presenting this paper in 2000, IEEE and IEC standards have emerged to address the need for substation-hardened communications and networking devices, and new products, with previously unavailable features, are available to apply in substation networks. In particular, new Ethernet switches have evolved to not only support the interleaved conversations inherent in Ethernet, but also perform information processing tasks, including the following:

- Segregation, defined in IEEE 802.1q.
- Prioritization, defined in IEEE 802.1p.
- Store and forward, similar to communications processors.
- Rugged construction, defined in IEEE 1613.

II. Serial Network Background and Components

A. Topology

Substation integration engineers often implement systems built of distributed devices that, among other things, replace the functions of a remote terminal unit (RTU). They use serial data links to communicate with protective relays and other IEDs. They typically connect each serial device to a station information processor with a point-to-point serial link to achieve higher reliability and data throughput, easier application of fiber optics, and lower cost than other serial network topologies [3]. These same network connections provide engineering access for settings maintenance and to retrieve data for post-event analysis. The serial ports are intrinsic to the relays and do not have a separate MTBF calculation.

Relay-to-relay communications are implemented using dedicated serial links performing IED-to-IED messaging, independent of the SCADA and engineering access network. The implementation of the Serial IED-to-IED messaging as a point-to-point protocol closely matches the implementation of several synchrophasor protocols. Synchrophasors are becoming a very important consideration for future wide area protection and control strategies. The fact that the Serial IED-to-IED protocol and synchrophasor protocols are implemented as point-to-point connections will simplify installations that include both protocols. This functional similarity makes the implementation, design, and troubleshooting of the combined protocols more compatible.

B. Information Processors

An information processor collects data from all of the local devices, creates a substation database, and serves the data to all local and remote data consumers. Information processors need to meet the same specifications as other communications equipment in the substation. In serial networks, information processing is accomplished with communications processors or rugged computers with appropriate software.

III. Ethernet Background and Components

A. Network Representation

Often, Ethernet networks are inaccurately but very simply depicted as a single line with intersecting short lines connected to each device. This oversimplification is intended to illustrate the logic of connecting to the "ether" but has the effect of hiding from view very important and necessary devices and connections. Modern Ethernet networks function adequately for substation automation only with the addition of many more components and connections than are visible in this abstraction. The designer must understand and document all Ethernet components, specialized configuration of these components, and interconnections to analyze system reliability and to design, procure, install, and maintain the network.

B. Media

Most Ethernet networks employ either specialized twisted-pair copper wiring or optical fiber. Standard designators identify the data rate and the medium compatible with an Ethernet port.

A data-rate indicator commonly precedes the medium designation, indicating a rate of 10, 100, or 1000 megabits per second. For higher speed networks operating at 10 gigabits per second, the IEEE uses the designation "10GBASE."

Many older cable types were used in the past. At this time, the physical Ethernet networks that are most likely to be employed in substation networks are 100BASE-T and 100BASE-FX, as shown in the first two lines of Table I.

TABLE I
ETHERNET MEDIA DESIGNATIONS

Designator	Data Rate	Medium	Defining Standard
10/100BASE-T	10 or 100 Megabits per second	Twisted pairs of copper cable CAT-5	IEEE 802.3u
100BASE-FX	100 Megabits per second	Fiber-optic cable at 1300 nm wavelength	IEEE 802.3u
1000BASE-T	1 Gigabit per second	Twisted pairs of copper cable CAT-5, CAT5e, or CAT-6	IEEE 802.3ab
1000BASE-SX	1 Gigabit per second	Multimode fiber-optic cable at 850 nm wavelength	IEEE 802.3z
1000BASE-LX	1 Gigabit per second	Single-mode fiber-optic cable at 1270–1355 nm wavelength	IEEE 802.3z

Engineers often select fiber-optic cable for substation monitoring and control system communications because it has the following features and capabilities:

- Isolates equipment from hazardous and damaging ground potential rise.
- Is immune to radio frequency interference and other electromagnetic interference.
- Eliminates data errors caused by communications ground-loop problems.
- Allows longer signal paths than copper connections.

Copper connections are sometimes selected for locations where the items above do not apply. This is because generally copper costs less than fiber, the equipment connected by copper costs less than equipment connected by fiber, and fewer special tools and skills are required to terminate copper.

C. Ethernet Hubs

A hub is a relatively simple multiport device that rebroadcasts all data that it receives on each port to all remaining ports. It operates at the Physical layer of the OSI network model, so it does not use any of the data to determine routing actions [4]. Hubs are not recommended for electric substation applications and are not generally applied. This is because switches use the bandwidth more effectively, and switches block broadcast data storms. The Ethernet phenomenon "broadcast data storm" occurs if an Ethernet network interface fails and continuously broadcasts messages, corrupting communications with any recipient of the data. Switches and routers can prevent a broadcast data storm from influencing communications on other segments of the network, but no data can be retrieved from the failed segments. Shared hubs pass on the broadcast data storm and impact other connected segments. Presently, the only recommended use for a hub is within conformance testing of IEDs where test cases require that no network device modify or influence the device under test or the network traffic.

D. Ethernet Switches

A switch is an intelligent multiplexing device that monitors the data received on one port to determine its disposition. A switch operates at the Data Link layer of the OSI network model. If a data packet is incomplete or indecipherable, the switch ignores it and does not rebroadcast it. If a data packet is intact, the switch rebroadcasts it to another port, based on the addressing data included in the packet and the addresses associated with each port of the switch. As mentioned previously, Ethernet switches now must be configured in concert with other information processors, they must exhibit rugged construction, and they must specifically perform the following four tasks.

1. Interleaved conversations
2. Message and IED segregation
3. Message prioritization
4. Message store and forward

E. Media Converters

Individual IEDs may have copper Ethernet ports, but the station network might use optical fiber. A media converter connects portions of the network that use different media.

F. Routers

A router is an intelligent multiplexing device used to connect two networks together. It can be a complex device with many features. It operates at the Network layer of the OSI network model. A router is programmed to ignore intrasegment traffic and to route intersegment traffic to the appropriate destination segment. Commercial Ethernet routers have an average MTBF of 9.5 years.

G. IED Ethernet Interfaces

An IED Ethernet interface is an intelligent device that connects an IED to an Ethernet network. Each device that is connected to the Ethernet must have an Ethernet interface that includes transceiver technology to match the network speed and medium. IED Ethernet interfaces generally fall into two categories: board level and port level. Board-level interfaces connect to the IED messaging through a special-purpose board-level connection. Port-level interfaces connect to general-purpose messaging connections and, in some cases, convert from a different medium to Ethernet.

H. Information Processor

In Ethernet networks, the information processing is generally accomplished with a rugged computer and one or more Ethernet switches. As part of its purpose, an information processor collects data, acting as a client of these data, from all of the local devices and creates a substation database. Once created, a server function serves these data from the database to other applications within the information processor or remote from it. Often, a local human-machine interface graphics package uses data from this database. Though less flexible, some specially developed applications directly connect client and server functionality without a database in between. Client and server functions operate at the Application layer of the OSI model. Information processors need to meet the same specifications as other communications equipment in the substation, so generally they are implemented with computers that are specifically designed to meet these requirements.

IV. Device Unavailability and Fault Tree Summary

An explanation of device unavailability and fault tree construction is included in [3]. Reference [5] is a handbook covering these subjects. At a summary level, fault trees predict system unavailability by providing the following time measurements:

- MTTR: the mean time to detect and repair a failure; 48 hours for the devices in these examples.
- MTTF: the mean time to fail.
- MTBF: the mean time between failures, defined as the sum of MTTR and MTTF. For the devices discussed in this paper, MTTF is much larger than MTTR, so we approximate MTBF as equal to MTTF.

Unavailability is the probability that a device will be unavailable to perform the functions vital to system operation and is the ratio of MTTR to MTBF.

Table II shows the average MTBF and unavailability for relevant instrumentation, control, and networking devices. Several commercial-grade devices are shown for comparison, but substation-grade devices are used in the examples. Unavailabilities are calculated from the MTBF and MTTR, as shown in (1).

Data from a manufacturer's experience show an MTBF of 335 years for a communications processor designed for a substation environment. Assuming 48 hours to detect and repair a failure (MTTR), the unavailability "q" is:

$$q = \left(\frac{48 \text{ hours}}{335 \text{ years} \cdot 365 \text{ days / year} \cdot 24 \text{ hours / day}} \right) = 16.35 \cdot 10^{-6} \quad (1)$$

$$q \cong 16 \cdot 10^{-6}$$

The MTBF values in Table II are based on averaged data from one or more manufacturers of specific products in each category. When evaluating actual systems, use the MTBF of the actual components proposed for each alternative.

TABLE II
APPROXIMATE COMPONENT UNAVAILABILITIES

Component	MTBF (years)	Unavailability (multiply by 10^{-6})
Substation-Grade IED Ethernet Interface	1320	4
Substation-Grade Fiber-Optic Transceiver	600	9
Substation-Grade Communications Processor (used as an information processor)	335	16
Substation-Grade Protective Relay IED Hardware	150	37
Substation-Grade Ethernet Switch With Dual Power Supply	106	52
Substation-Grade Ethernet Switch	57	96
Substation-Grade Computer (used as an information processor)	50	110
Substation-Grade Ethernet Router	40	137
Commercial Ethernet Router With Dual Power Supply	35	156
Industrial PC (used as an information processor)	14	391
Commercial Ethernet Switch	11.5	477
Commercial Media Converter	11.5	391
Commercial Ethernet Router	9.5	577
Commercial PC (used as an information processor)	4	1370

Note: The most reliable components have the smallest unavailability numbers.

V. EXAMPLE COMPARISONS FOR INSTRUMENTATION AND CONTROL

A. Functional Requirements

The functional requirements for the example I&C system are as follows:

- Use the protective relays for the I/O interface to the station equipment.
- Provide operational data and control for a SCADA system acting in lieu of an RTU.
- Implement relay-to-relay communication for backup bus protection.
- Facilitate engineering access to retrieve timetagged oscillographic event reports and sequential event records and maintain relay settings.

B. Example Station Description

Consider a substation with two line connections, two transformers, a high-side and a low-side bus, and four feeders, as shown in the one-line diagram of Fig. 1.

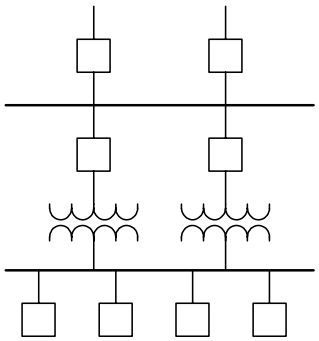

Fig. 1. Example Station One-Line Diagram

The protection for each transmission line is a dual-primary scheme, using a distance operating principle for Main 1 and line-current differential protection for Main 2. The relay usage is summarized in Table III.

TABLE III
PROTECTIVE RELAYS

Relay	Quantity
Transmission line distance protection	2
Transmission line-current differential protection	2
Transformer protection	2
Bus protection	2
Feeder protection	4
Total	12

The availability analyses focus on the differences between the systems. References [3] and [6] describe additional items that impact overall instrumentation and control availability. Specifically in this paper, we do not include the impacts of the station battery, instrument transformers, communications cable failures, backhoe operators digging through cables, or WAN failures because they represent comparable risks in all of the alternatives.

C. Serial Star Network

A block diagram of a star network is shown in Fig. 2. A serial communications link (solid lines) connects each relay to the communications processor. For the relay-to-relay backup scheme, serial links (dotted lines) connect the relays. An Ethernet connection (dashed line) connects to the SCADA system via a WAN.

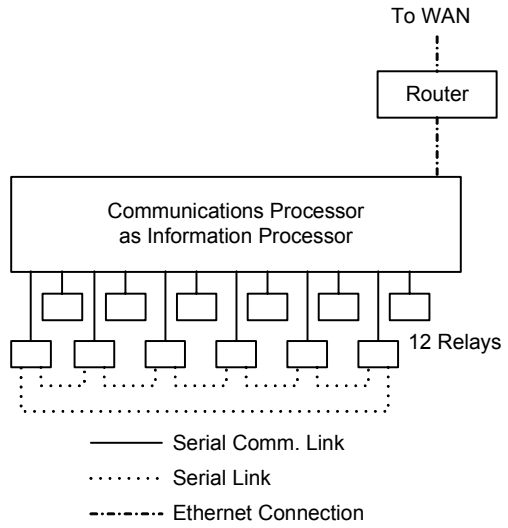

Fig. 2. Serial Star Network Block Diagram

When you know the unavailability for each component of a system, fault trees are useful to predict the overall system unavailability [3]. Use OR gates to sum the unavailabilities when failure of any of the devices causes a system failure, and use AND gates to calculate the product of unavailabilities when all of the failures must occur for the system to fail. The fault tree shown in Fig. 3 depicts the system unavailability analysis. The top event of the tree indicates that the computed unavailability is the probability that an operator accessing the substation systems would not be able to retrieve all of the data, would be prevented from control, or an engineer would not be able to access a relay to retrieve data or maintain settings.

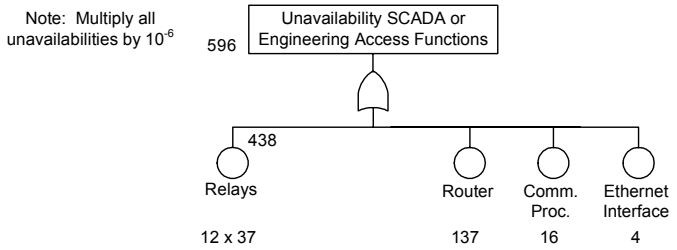

Fig. 3. Serial Star Network Fault Tree

A failure of the communications processor, Ethernet interface, router, or any relay will cause the top event. The summed unavailability is $596 \cdot 10^{-6}$. $1–(596 \cdot 10^{-6})$ is the system availability or 99.9404%.

If a substation-grade computer is used in the star network instead of a communications processor, then subtract the unavailability of the communications processor and its Ethernet interface and add the unavailability of the rugged computer, yielding a summed unavailability of $685 \cdot 10^{-6}$. The availability is $1–(685 \cdot 10^{-6})$ or 99.9315%.

For the relay-to-relay protection links, only six relays are involved. The summed unavailability is $219 \cdot 10^{-6}$. The availability is $1–(219 \cdot 10^{-6})$, or 99.9781%.

D. Switched Ethernet LAN

A block diagram for an Ethernet substation LAN is shown in Fig. 4.

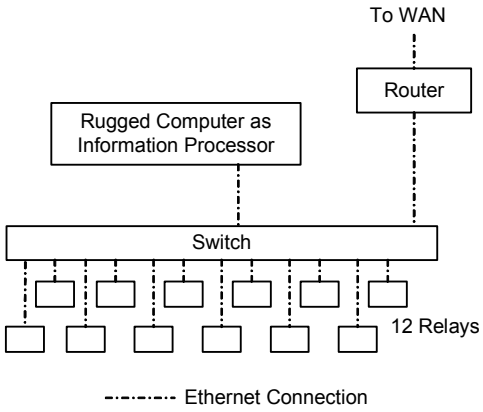

Fig. 4. Switched LAN Block Diagram

The fault tree shown in Fig. 5 depicts the system unavailability analysis. The top event of the tree indicates that the computed unavailability is the probability that an operator accessing the substation systems would not be able to retrieve all of the data, would be prevented from control, or an engineer would not be able to access a relay to retrieve data or maintain settings.

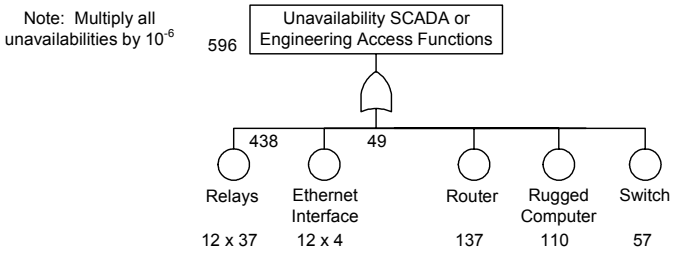

Fig. 5. Switched LAN Fault Tree Diagram

A failure of the router, rugged computer, switch, or any relay or Ethernet interface will cause the top event. The summed unavailability is $831 \cdot 10^{-6}$. $1–(831 \cdot 10^{-6})$ is the system availability or 99.9169%.

The biggest contributor to failures in the switch used in the example is the power supply. If a dual power-supply switch is used, with an unavailability of $106 \cdot 10^{-6}$ instead of $57 \cdot 10^{-6}$, the overall summed unavailability is $814 \cdot 10^{-6}$. The availability is $1–(814 \cdot 10^{-6})$ or 99.9186%.

For the relay-to-relay protection links, the switch, six relays, and six Ethernet interfaces are involved. The summed unavailability is $340 \cdot 10^{-6}$. The availability is $1–(340 \cdot 10^{-6})$ or 99.9660%.

E. Availability Comparison

Table IV summarizes the availabilities of four system architectures for two top events. The predicted annual hours out

of service is the unavailability multiplied by the number of hours in a year.

TABLE IV
COMPARATIVE SYSTEM AVAILABILITY

Alternative	Availability %	Predicted Annual Hours Out of Service
SCADA and Engineering Access for 12 Relays		
Serial Star Network: Comm. Processor	99.9404	5.2
Serial Star Network: Rugged Computer	99.9315	6.0
Ethernet LAN With Dual Power Switch	99.9214	6.9
Switched Ethernet LAN	99.9169	7.3
Relay-to-Relay Communications for 6 Relays		
Serial Point-to-Point	99.9781	1.9
Switched Ethernet LAN	99.9660	3.0

F. Cost Comparison

The first row of Table V summarizes the approximate costs of the components and software for three network types.

The labor and travel costs to repair failures in ten years of operation are shown in the second row. Because equipment repair or replacement is required on failure of any device regardless of redundancy, the top event of, "Any Equipment Fails," yields a fault tree with a single OR gate with all equipment unavailabilities as its inputs. Statistically, the repair cost is most useful when considering a population of ten or more stations because a single system will not experience a fractional number of failures.

The third row shows the approximate protocol mapping and integration costs. The serial star network integration costs are based on using the native protocols of the relays for the connection to the communications processor or rugged computer and relay-to-relay communications, plus DNP3 LAN/WAN for the SCADA link. The switched Ethernet LAN is based on using IEC 61850 for communication with the relays and IEC 61850 GOOSE messages for relay-to-relay communication. The labor hour estimates were provided by integration engineers who have delivered similar systems of each type, using a per hour rate of $110.

TABLE V
COST COMPARISON OF VARIOUS SYSTEMS

	Serial Star With Comm. Processor	Serial Star With Rugged Computer	Switched Ethernet LAN
Initial Equipment	74,000	76,000	104,000
Ten-Year Repair	1,380	1,380	1,990
Protocol Mapping/Integration	4,400	7,700	35,200

Note: All costs are shown in U.S. dollars.

G. IED-to-IED Communications Comparison

The serial networks use dedicated links for relay-to-relay communication via an IED-to-IED protocol within the station. This Serial IED-to-IED protocol rapidly exchanges redundant data payloads between the IEDs constantly and, in doing so, also calculates channel availability and alarms for problems. The switched LAN system in this example uses IEC 61850 GOOSE messages.

1) Speed of Logic-to-Logic Status Transfer Between IEDs

The IEC 61850 standard defines speed criteria that cannot be easily measured. Therefore, it is not presently feasible to test and verify the transmit time performance classes as described in the standard. Instead, it is possible to easily measure the transfer time, which includes the transmit time plus the time to process and timestamp the transmitted data. This transfer time is what network designers are actually concerned about because it represents the performance of communications in actual use. Data element state changes are timestamped and logged as sequential events records (SER). In IEDs with clocks synchronized to the same time reference and that create accurate timestamps, SER are used to calculate transfer time, which includes transmit time plus processing time in the receiving IED. Therefore, communications designs were compared on their ability to transfer information to a peer and have that peer process it. This was detected by creating an SER1 in IED1 when the state change occurs and the associated message is sent to another IED, IED2. IED2 creates SER2 once it receives and processes the state change, inverts it, creates SER3, and then sends a new message to IED1, which creates SER4 when it sees the state change. The difference between SER1 and SER2 in IEDs with synchronized clocks represents the transmission and processing time of one message, as does the difference between SER3 and SER4.

At 38,400 bps, the average time difference between status transfers, SER2–SER1 and SER4–SER3, for the Serial IED-to-IED protocol is consistently between 3 and 4 ms. The time difference for GOOSE is 4 ms. Subtracting the receiving IED processing time from these transfer time measures reveals a transmit time for both protocols that meets even the most stringent performance class. However, keep in mind that this testing demonstrates a single-vendor implementation of GOOSE that is satisfactory. Other vendor device performances will vary based on hardware and software implementation and have been observed to not meet the performance classes.

2) Dependability of Status Message Transfer Between IEDs

The Serial IED-to-IED protocol messages are checked several ways to ensure data reliability. Messages are constantly broadcast between IEDs that then acknowledge delivery, check message security, and check each byte of the received messages for parity, framing, and overrun errors. If any of the protocol security checks fail, the start and end times of the disruption are recorded; the difference is calculated as the disruption duration, which triggers a threshold alarm. The duration is set based on the existing communications system performance to avoid nuisance alarms. The Serial IED-to-IED channel unavailability is the ratio of the amount of time the channel is unavailable to pass messages (determined as the sum of all disruption durations) to the total recording interval

time. This is calculated by dividing the aggregate of all outage durations by the total time span for a recording period and is presented as ppm unavailability.

The Ethernet-based IEC 61850 protocol does not currently include methods to automatically detect GOOSE delivery failures or include GOOSE communications performance and availability calculations. This is because messages with new data are transmitted by exception and, when no data are changing, messages with stale data are transmitted at an infrequent rate to support "heartbeat" or "watchdog" alarm detection. Due to the potential importance of each GOOSE message and the possibility of delay or incomplete transmission inherent in Ethernet networks, the IEC 61850 standard requires that each IED send multiple repetitive GOOSE messages in fast succession to increase the likelihood of message delivery.

The GOOSE protocol is presently designed without a message receipt acknowledgment mechanism; therefore, GOOSE message channels cannot be monitored for availability or dependability. Each successive GOOSE message is given a sequence number and a time-to-live value to aid receiving IEDs in message processing. The time-to-live value is compared to the time duration difference since the message was created. If the duration difference is larger than the time-to-live value, the sending IED considers the message "old." The receiving IED can choose to use this indication as a validity check before it acts on data in the received message.

Although the GOOSE protocol does not provide message receipt acknowledgment, custom logic available in IEDs from some vendors can be used to accomplish this function. By configuring the IEDs to repeatedly and cyclically send GOOSE messages and monitor the receipt of each message, the IED logic can calculate channel performance [7].

Complete verification of correct operation of the GOOSE messages on the Ethernet network requires diagnostics in the IEDs. Testing for this paper as well as years of experience in commissioning Ethernet systems demonstrate that it is essential that the IEDs provide diagnostics to complement analysis available via network analyzers. The necessary IED status and messaging status information should be available directly from the in-service IED. Listed below is status information that proved essential in the IEDs tested for this paper.

- Message received out of sequence
- IED configuration revision mismatch detected
- IED not yet commissioned
- IED in test mode
- Message is corrupted
- Message time to live has expired
- Host disabled/not responding

3) Complexity of Status Message Transfer Method Between IEDs—Message Processing [8]

The Serial IED-to-IED protocol was designed specifically for point-to-point data exchange between power system IEDs. The designers combined their skills in the art of protecting and automating power systems with their knowledge of the parameters of IED development to create a very concise and streamlined process. This process is detailed as follows:

a) Transmit Serial IED-to-IED Message

1. Detect change in relay logic intended for transmission.
2. Update new message with data.
3. Encode message.
4. Transmit message.

The quantity of lines of code (LOC) required to perform a function represents the complexity of the development, testing, and maintenance of the process. The total LOC required to transmit a Serial IED-to-IED message, Steps 2–4, is 356.

b) Receive Serial IED-to-IED Message

1. Receive message.
2. Validate message.
3. Decode message.
4. Transfer contents to host logic.
5. Detect resultant change in relay logic.

The total LOC required to receive a Serial IED-to-IED message, Steps 1–4, is 360.

GOOSE messages were designed to serve many purposes on an Ethernet network based on the constraints of Ethernet interface hardware and network equipment. This process is detailed as follows:

c) Transmit GOOSE Message

1. Detect and forward change in relay logic intended for transmission via GOOSE.
2. Detect this forwarded change in GOOSE interface.
3. Store new value for changed item.
4. Queue payload for use in GOOSE.
5. Determine changed data and update GOOSE.
6. Determine changed qualities and update GOOSE.
7. Update GOOSE message with date and timestamp.
8. Decompose message data to primitive types.
9. Encode contents using abstract syntax notation (ASN.1).
10. Encode GOOSE message.
11. Send GOOSE message.
12. Manage Ethernet transmit buffers.

The total LOC required to transmit a GOOSE message, Steps 2–12, is 4430.

d) Receive GOOSE Message

1. Manage Ethernet receive buffers.
2. Receive Ethernet frame.
3. Identify that content of Ethernet frame is a GOOSE message.
4. Push GOOSE message to queue.
5. Retrieve GOOSE message descriptor.
6. Decode GOOSE message.
7. Validate GOOSE message global quality.

8. Extract data from GOOSE message.
9. Validate GOOSE content quality.
10. Release decoded GOOSE data and Ethernet frame.
11. Update the GOOSE time-to-live timers.
12. Transfer GOOSE contents to host.
13. Transfer bit to host logic.
14. Detect change in relay logic received via GOOSE.

The total LOC required to transmit a GOOSE message, Steps 1–13, is 3590.

4) Complexity of Status Message Transfer Method Between IEDs—Message Size

Another measure of complexity is the size in bytes of the total message string necessary to move data between IEDs. It should be apparent that the message security, described previously, is useful only to minimize the risk of an IED accepting a corrupted message. However, in point-to-point applications, the more important, and often overlooked, measure is dependability, knowing that the correct data and message will get through when necessary. Message overhead complexity, as a result of message flexibility and message size, is inversely proportional to the ability to send and parse an uncorrupted peer-to-peer message.

The Serial IED-to-IED message, due to its concise design and transfer, is four bytes in length. GOOSE messages vary in size based on their flexible payload. However, a GOOSE message requires roughly 200 bytes to transfer a single Remedial Action Scheme (RAS) bit, which is 50 times larger than a Serial IED-to-IED message. It is, therefore, more susceptible to message corruption as a result of communications channel errors. The repetitive delivery of both message types can alleviate this concern. The GOOSE message transfers a payload of approximately 150 bits, compared to 8 bits for a Serial IED-to-IED message. If you use 3 bits for each GOOSE bit to increase the GOOSE message dependability, the GOOSE message has an effective payload of 50 bits.

5) Complexity of Status Message Transfer Method Between IEDs—Configuration Effort

Still another measure of complexity is the quantity of settings required to configure the exchange of a status bit between two peer IEDs. The Serial IED-to-IED messaging was designed to exchange bits of information between IEDs as soon as the protocol is enabled in the IED. Therefore, after four simple settings in two IEDs, the IEDs exchange two sets of eight bits over two channels. Reliability and channel monitoring alarms and statistics will be calculated automatically.

GOOSE requires a minimum of fourteen settings in each of the two IEDs to begin sending a single bit from one IED to the other. More settings are required if the payload is larger than one bit. Twenty-eight settings are required to exchange a bit pair (i.e., one bit from IED1 to IED2 and a different bit from IED2 back to IED1). Then additional logic settings must be created to simulate the automatic reliability and channel monitoring alarms and statistics of the Serial IED-to-IED protocol.

Though configuration software may automatically set some of the twenty-eight settings, they are each required in order to exchange bits. This represents a much more complex configuration with more opportunity for error and, therefore, more complex troubleshooting.

TABLE VI
SYSTEM COMPARISON OF IED-TO-IED COMMUNICATIONS

	Serial Point-to-Point	**Switched Ethernet LAN**
Availability	99.9781%	99.9660%
Configuration Effort/Device	4 Settings	28 Settings
Control Transfer Speed	3–4 ms	4 ms
Channel Monitoring	Built-in	Via custom logic settings
Message Payload Repetition	Built-in	Custom Logic
Complexity Reflected as Required Lines of Code (LOC)	726 LOC	8,020 LOC
Complexity Reflected as Message Size for 1 Peer-to-Peer Status Bit	4 Bytes	200 Bytes
Effective Payload	8 Bits	50 Bits (using 3 GOOSE bits per payload bit)

6) System Cryptography Analysis

Cryptographic features necessary to provide cybersecurity of the protocols associated with cyberassets include confidentiality, message integrity, and connection authentication.

As described previously, the Serial IED-to-IED protocol is easily communicated over an assortment of communications systems. Due to the concise messaging and the fact that the physical and logical connections are true point-to-point, cryptography is very easily added to this protocol. Bump-in-the-wire cryptography devices quickly and inexpensively add confidentiality (via encryption) and connection authentication (via key exchange) to the messages without impacting the throughput time performance of the RAS protocol messages [9]. Integrity of the messages is assured by the physical point-to-point nature of the connections and the payload redundancy designed into the protocol.

GOOSE, as with all protocols within the IEC 61850 standard, does not have security features. A separate standard, IEC 62351, is now under development to create security methods to add to networks using this and other protocols. Therefore, Ethernet security methods are the only tools available to add cryptography to GOOSE traffic. The method available today is to segregate traffic and allow only authorized endpoints to connect to the network. The switches used are capable of grouping subsets of their ports into virtual broadcast domains isolated from each other. These domains are commonly known as virtual LANs (VLANs).

The VLAN concept is akin to other concepts in the networking world where traffic is identified by the use of a tag or label. Identification is crucial for switches to isolate ports and properly forward the traffic received. Lack of identification is sometimes a cause of insecurity and needs to be avoided [9].

It is essential, therefore, that network designers choose and correctly implement switches that support VLAN tagging for performance as well as security.

Using VLAN, GOOSE traffic authentication is provided if no other endpoints are successfully connected to the virtual network. If this is true and if a packet's VLAN identification cannot be altered after transmission from its source and is consistently preserved from end to end, then VLAN-based authentication is no less reliable than physical security. VLAN does not provide confidentiality of the messages or integrity of the contents.

Also, recommended best practice dictates that two remote LANs not be directly connected to one another over an untrusted link. However, GOOSE messages cannot be routed over a WAN. A secure method for sending GOOSE messages between substations is passing them over a private network between the stations.

VI. Conclusions

As expected, between the years 2000 and 2007, advancements have improved the feasibility of applying Ethernet networks in electrical substations.

1. Standards organizations and manufacturers have responded to the need for substation-grade networking components that withstand the harsh electrical conditions of substations and exhibit much higher reliability than commercial and most industrial components.
2. For the example substation and network alternatives examined in this paper, star serial networks continue to be more reliable than Ethernet networks, but the reliability gap between the two approaches is smaller now than it was in 2000. When using an Ethernet network for mission-critical SCADA or protection, it is worth the small incremental cost of a higher-reliability switch that includes dual power supplies.
3. Even with advancements in computer-aided engineering tools, integrating an IEC 61850-based system still requires significantly more labor than other approaches.
4. More and more electric utilities, integrators, and manufacturers are using or providing IEC 61850 systems and products, and this will continue to drive improvements in integration tools. These tools need to advance for the industry to realize the promise of IEC 61850, which is to reduce the effort to integrate devices from many suppliers.
5. For relay-to-relay communications, direct communications external to a LAN are more reliable than GOOSE over a LAN, are less complex, and depend on far fewer settings. Performance measures of transfer speed indicate that in operation, either approach performs sufficiently.
6. This paper provides an example evaluation using generalized or averaged values for MTBF and costs, for a specific four-feeder substation. Choose top events for the fault trees that yield the unavailability of the system to accomplish a well-defined task or group of tasks. For other specific applications, use the actual MTBF data and costs for the components under consideration, and follow a similar process to evaluate the actual alternatives.
7. Practice to date has demonstrated that it is essential that the IEDs provide diagnostics to complement analysis available via network analyzers. The necessary IED status and messaging status information should be available directly from the in-service IED.
8. The implementation of the Serial IED-to-IED messaging as a point-to-point protocol closely matches the implementation of several synchrophasor protocols. Synchrophasors are becoming a very important consideration for future wide area protection and control strategies. The fact that the Serial IED-to-IED protocol and synchrophasor protocols are implemented as point-to-point connections, instead of broadcast, will simplify installations that include both protocols. This functional similarity makes the implementation, design, and troubleshooting of the combined protocols more compatible.

VII. References

[1] IEC 60870-4, Telecontrol Equipment and Systems Part 4: Performance Requirements.

[2] G. W. Scheer, D. J. Dolezilek, "Comparing the Reliability of Ethernet Network Topologies in Substation Control and Monitoring Networks," Proceedings of the Second Annual Western Power Delivery and Automation Conference, Spokane, WA, April 5–7, 2000.

[3] G. W. Scheer, "Answering Substation Automation Questions Through Fault Tree Analysis," Proceedings of the Fourth Annual Texas A&M Substation Automation Conference, College Station, TX, April 8–9, 1998.

[4] D. Woodward, "The Hows and Whys of Ethernet Networks in Substations," Proceedings of the Third Annual Western Power Delivery and Automation Conference, Spokane, WA, April 10–12, 2001.

[5] N. H. Roberts, W. E. Vesely, D. F. Haasl, and F. F. Goldberg, "Fault Tree Handbook," NUREG-0492m U.S. Nuclear Regulatory Commission, Washington, DC, 1981.

[6] G. W. Scheer, "Comparison of Fiber-Optic Star and Ring Topologies for Electric Power Substation Communications," Proceedings of the First Annual Western Power Delivery and Automation Conference, Spokane, WA, April 6–8, 1999.

[7] V. Skendzic and A. Guzmán, "Enhancing Power System Automation Through the Use of Real-Time Ethernet," Proceedings of the Eighth Annual Western Power Delivery Automation Conference, Spokane, WA, April 2006.

[8] M. Gugerty, R. Jenkins, and D. J. Dolezilek, "Case Study Comparison of Serial and Ethernet Digital Communications Technologies for Transfer of Relay Quantities," Proceedings of the 33rd Annual Western Protective Relay Conference, Spokane, WA, October 17–19, 2006.

[9] "Virtual LAN Security Best Practices," VLAN Security White Paper, <www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml>.

VIII. Biographies

Gary W. Scheer received his B.S. in Electrical Engineering from Montana State University in 1977. He worked for the Montana Power Company and the MPC subsidiary, The Tetragenics Company, before joining Schweitzer Engineering Laboratories, Inc. in 1990 as a development engineer. He has served as Vice President of the Research and Development Division and of the Automation and Engineering Services Division of SEL. Mr. Scheer is now a senior engineer in the Marketing Department. His biography appears in Who's Who in America. He holds two patents related to teleprotection. He is a registered professional engineer and member of the IEEE and the ISA.

David J. Dolezilek received his BSEE from Montana State University in 1987 and is now the technology director of Schweitzer Engineering Laboratories, Inc. He is an electrical engineer with management and development experience in electric power protection, integration and automation, communications, control systems, SCADA and EMS design, and implementation. He is the author of numerous technical papers and continues to research and write about innovative design and implementation affecting our industry. Dolezilek is a patented inventor and participates in numerous working groups and technical committees. He is a member of the IEEE, the IEEE Reliability Society, CIGRE working groups, and two International Electrotechnical Commission (IEC) Technical Committees tasked with global standardization and security of communications networks and systems in substations.

20070524
TP6273-01