# Practical Considerations for Ethernet Networking Within Substations

Shawn Coppel
*American Electric Power*

Timothy Tibbals and Adrian Silgardo
*Schweitzer Engineering Laboratories, Inc.*

Published in
SEL *Journal of Reliable Power*, Volume 3, Number 2, August 2012

Originally presented at the
10th Annual Western Power Delivery Automation Conference, April 2008

# Practical Considerations for Ethernet Networking Within Substations

Shawn Coppel, *American Electric Power*
Timothy Tibbals and Adrian Silgardo, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—A growing number of electric utilities are applying or evaluating Ethernet networks for substation instrumentation and control (I&C). Interest in Ethernet is driven, in part, by the desire to achieve faster and lower-cost substation integration. This is achieved by reducing the labor required to integrate monitoring and control devices for substation and feeder equipment using standardized interfaces (Ethernet) and protocols (IEC 61850). If devices from multiple vendors comply with the rules (interoperability), special integration labor for each device is reduced or eliminated.**

**This paper looks at the new capabilities in substation automation, protection, and control made possible by native intersubstation Ethernet. It also discusses techniques to make the network secure and dependable, examines real-world examples, and presents considerations and issues that need to be addressed to create a successful, reliable Ethernet protection and data collection infrastructure.**

## I. Introduction

As the business sector Ethernet moves to gigabit-speed backbones, electric utilities are just beginning to realize the capabilities and benefits of Ethernet communications in the substation and control centers. Ethernet networks provide benefits and shortcomings compared to other approaches. It is essential to identify and understand these tradeoffs in order to make practical decisions for Ethernet applications. These tradeoffs drive the selection of system features and benefits, define the measures of success, and identify areas for improvement. This paper discusses and compares the contemporary, integrated communications topologies available to meet the instrumentation and control (I&C) demands of a typical substation.

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

We also discuss the reliability of these Ethernet systems using methods presented in previous papers [1] [2].

IEEE and IEC standards address substation-hardened communications and networking devices for application in substation networks [3] [4].

New Ethernet switches have evolved to support the features needed in the substation network and environment including segregation, prioritization, and rugged construction.

More recently, the security of networking and data communications has been a primary focus of utilities and the North American Electric Reliability Corporation (NERC). Requirements have been put into place to address the security of these critical infrastructures and assets. We discuss these requirements as they relate to the components and architecture of the substation Ethernet network.

## II. Ethernet Background and Components

### A. Network Representation

Often Ethernet networks are depicted as a single line with intersecting short lines connected to each device. Modern Ethernet networks function adequately for substation automation only with the addition of many more components and connections than are visible in this single line abstraction. The designer must understand and document all Ethernet components, specialized component configurations, 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 1,000 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, 10/100BASE-T and 100BASE-FX Ethernet networks are most likely to be employed in substation networks, 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 CAT 5 copper cable | IEEE 802.3u |
| 100BASE-FX | 100 megabits per second | Fiber-optic cable at 1,300 nm wavelength | IEEE 802.3u |
| 1000BASE-T | 1 gigabits per second | Twisted pairs of copper cable (CAT 5, CAT 5e, or CAT 6) | IEEE 802.3ab |
| 1000BASE-SX | 1 gigabits per second | Multimode fiber-optic cable at 850 nm wavelength | IEEE 802.3z |
| 1000BASE-LX | 1 gigabits per second | Single-mode fiber-optic cable at 1,270 to 1,355 nm wavelength | IEEE 802.3z |

Engineers often select fiber-optic cable for substation monitoring and control system communications to take advantage of the following features and capabilities:

- Isolates equipment from hazardous and damaging ground potential rise.
- Rejects 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 because, generally, copper costs less than fiber, the equipment connected by copper costs less than the equipment connected by fiber, and fewer special tools and skills are required to terminate copper cables.

### *C. 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 Open Systems Interconnection (OSI) network model data link layer. 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 address data included in the packet and the addresses associated with each port of the switch.

### *D. Media Converters*

Individual intelligent electronic devices (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.

### *E. 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 route intersegment traffic to the appropriate destination segment.

### *F. IED Ethernet Interfaces*

An IED Ethernet interface is an intelligent device that connects an IED to an Ethernet network. Each device 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 different mediums to Ethernet.

### *G. Information Processor*

In Ethernet networks, 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 sends these data from the database to other applications either within or outside the information processor. Often a local human-machine interface (HMI) 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 OSI network model application layer. Information processors need to meet the same specifications as other communications equipment in the substation, so they are usually implemented with computers that are specifically designed to meet these requirements.

### *H. Device Unavailability and Fault Tree Summary*

An explanation of device unavailability and fault tree construction is included in [5]. Reference [6] is a handbook covering these subjects. At a summary level:

- MTTR is the mean time to detect and repair a failure; 48 hours for the devices in these examples.
- MTTF is the mean time to fail.
- MTBF is 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 it is the ratio of MTTR to MTBF.

TABLE II
APPROXIMATE UNAVAILABILITIES OF SEVERAL COMPONENTS

| **Component** | **Unavailability (Multiply by $10^{-6}$)** |
|---|---|
| IED Network Interface | 4 |
| Protective Relay IED Hardware | 37 |
| Dual Power Supply Ethernet Switch | 52 |
| Ethernet Switch (Substation Hardened) | 96 |
| Information Processor (Rugged Computer) | 110 |
| Dual Power Supply Ethernet Router (Substation Hardened) | 156 |

**Note**: The more widely available components have the smallest unavailability numbers.

When you know the unavailability for each system component, you can apply fault tree analysis to model overall system reliability. 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. See Fig. 3 and Fig. 5 for examples of fault tree analyses.

## III. TOPOLOGY COMPARISONS FOR DATA ACQUISITION AND CONTROL

### *A. Introduction*

The following analyses are based on an example 138/69 kV substation with eight circuit breakers (shown in Fig. 1), full primary and backup protective relays on the high-side breakers, and single protection relays on the transformers and low-side breakers. This is a total of 12 protective relays. Each relay is equipped with an Ethernet interface. An information processor based on an industrial computer is included to provide HMI and other data clients. A router provides a connection between the substation local-area network (LAN) and a system wide-area network (WAN).

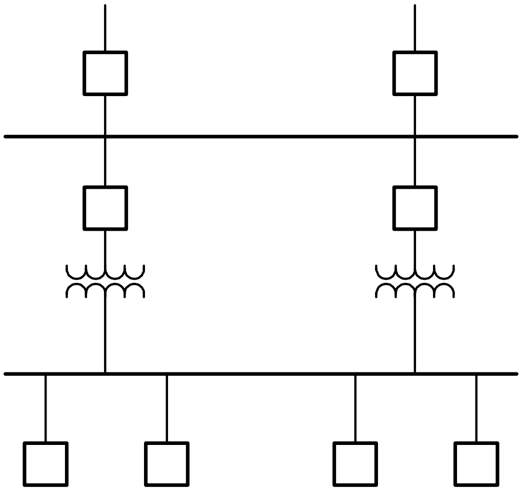


Fig. 1. Example System One-Line Diagram

The availability analyses in this paper focus on the differences between the systems. References [5] and [7] describe additional items that impact overall instrumentation and control availability. Specifically, we do not include the impacts of the station battery, instrument transformers, and fiber-optic cable digging errors because they represent comparable risks in all of the systems. The impact of software failures in the servers is not included, in part, because the systems share similar exposure, and because it is difficult to quantify software failure rates.

## B. Switched LAN

An Ethernet substation LAN using switches has a block diagram similar to Fig. 2. The fault tree for the switch-based system is shown in Fig. 3. The top event shown in the fault tree indicates the computed unavailability of access to supervisory control and data acquisition (SCADA) data or engineering access to any relay in the system. Failure of any item shown on the lower row of the fault tree will cause the top event. The combined unavailability of the switched LAN system is 831 • $10^{-6}$. The availability is (1).

$$1-831 \bullet 10^{-6} = 99.9169\% \tag{1}$$

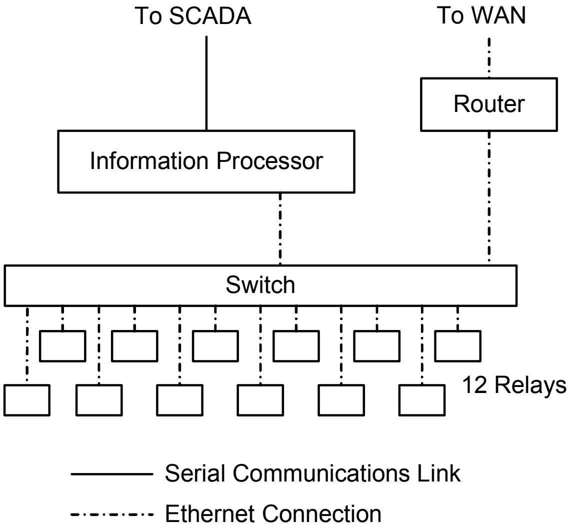
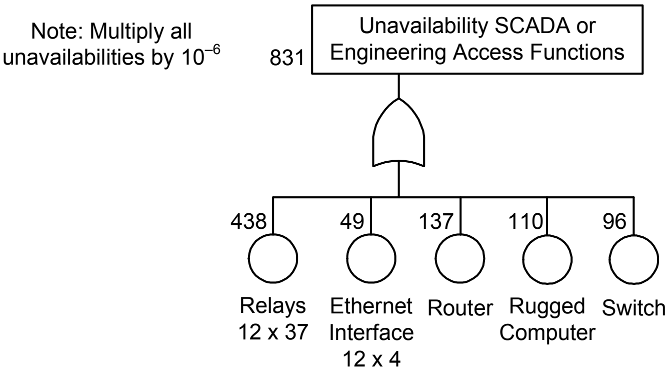


Fig. 2. Shared Switch LAN Block Diagram



Note: Multiply all unavailabilities by $10^{-6}$
831
Unavailability SCADA or Engineering Access Functions
438
49
137
110
96
Relays 12 x 37
Ethernet Interface 12 x 4
Router
Rugged Computer
Switch

Fig. 3. Switch Fault Tree

The largest contributor to the switch used in the example shown in Fig. 2 is the power supply. If a dual power supply switch is used, the overall summed unavailability improves to 736 • $10^{-6}$. The availability is (2).

$$1-736 \bullet 10^{-6} = 99.9214\% \tag{2}$$

### *C. Redundant Switched LAN*

The block diagram for a substation with redundant switched LANs is shown in Fig. 4. The fault for the redundant switch system is shown in Fig. 5. The overall unavailability of the redundant switched LAN is $624 \bullet 10^{-6}$, which is the sum of the protection network, server, and router unavailabilities. The availability is (3).

$$1 - 624 \bullet 10^{-6} = 99.9376\% \qquad (3)$$

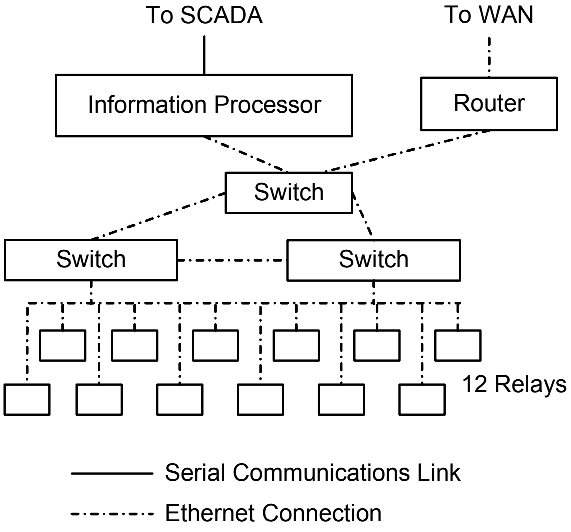


Fig. 4. Redundant Switch Block Diagram

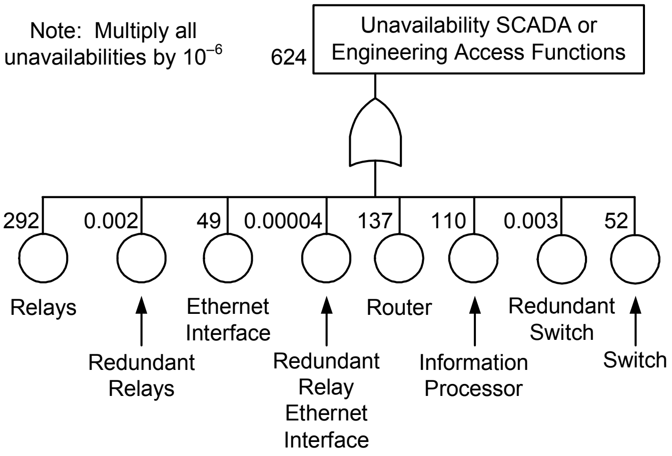

Note: Multiply all unavailabilities by $10^{-6}$
624
Unavailability SCADA or Engineering Access Functions
292
0.002
49
0.00004
137
110
0.003
52
Relays
Redundant Relays
Ethernet Interface
Redundant Relay Ethernet Interface
Router
Information Processor
Redundant Switch
Switch

Fig. 5. Redundant Switch Fault Tree

### *D. Redundant Servers, Routers, and Switches (LAN)*

Rather than replicating the entire network, a designer can split the communications network into primary and backup networks, which are connected to their respective primary and backup protection systems. This includes adding primary and backup protective relays to the transformer and low-side breakers that were not part of the previous examples. The primary and backup systems each have an unavailability of $624 \bullet 10^{-6}$. The combined system unavailability is $(624 \bullet 10^{-6})^2$ or $0.389 \bullet 10^{-6}$. The availability is (4).

$$1 - 0.389 \bullet 10^{-6} = 99.99996\% \qquad (4)$$

### *E. Availability Comparison*

Table III summarizes the connection topology availabilities discussed. The predicted annual hours out-of-service is the unavailability multiplied by the number of hours in a year.

TABLE III
AVAILABILITIES OF SYSTEMS TO RETRIEVE ALL LINE DATA AND OPERATE ANY BREAKER

| **Ethernet LAN** | **Availability %** | **Predicted Annual Hours Out-of-Service** |
|---|---|---|
| Shared Switch | 99.9214 | 6.9 |
| Redundant Switches | 99.9376 | 5.5 |
| Redundant Servers, Routers, and Switches | 99.99996 | 0.003 |

The redundant switch systems exhibit better availabilities than the respective nonredundant systems. Fully separate systems with redundant servers, routers, and switches exhibit the best availability of all these systems.

### *F. Cost Comparison*

Data are provided in this section to aid in identifying the cost and availability tradeoffs for the LANs. Table IV summarizes the approximate costs of the Ethernet components of each LAN in descending order of equipment cost. The average equipment prices for the IED interfaces, fiber-optic cables, hubs, switches, routers, and servers are included in the equipment costs. The repair costs are summarized in the last column of Table IV and include labor and nonwarranty material costs for all of the predicted equipment failures in ten years.

TABLE IV
TYPICAL EQUIPMENT AND MAINTENANCE COSTS OF ETHERNET LANS

| **Ethernet LAN** | **Initial Equipment Cost ($)** | **Ten-Year Repair Cost ($)** |
|---|---|---|
| Redundant Servers, Routers, and Switches | 203,000 | 1,446 |
| Redundant Switches | 111,000 | 1,823 |
| Dual Power Supply Switch | 105,000 | 1,446 |

## IV. NETWORK ROUTING AND SECURITY

Ethernet on its own provides little security from malicious intruders from a larger corporate network. A cybersecurity appliance with IP routing, firewall, virtual private network (VPN), and intrusion detection system (IDS) is one of the ways to create an “electronic security perimeter” around the critical cyberassets of the substation, as required by NERC CIP-005-1.

The NERC cybersecurity goal is to ensure that all entities responsible for the reliability of the bulk of the North American electric systems identify and protect critical cyberassets that control or could impact the reliability of these systems.

There are many aspects of security defined by NERC, as shown in Table V.

Table V
NERC Cybersecurity Standards

| NERC Std # | Topic |
|---|---|
| CIP-002-1 | Critical Cyberasset Identification |
| CIP-003-1 | Security Management Controls |
| CIP-004-1 | Personnel and Training |
| CIP-005-1 | Electronic Security Perimeter(s) |
| CIP-006-1 | Physical Security |
| CIP-007-1 | Systems Security Management |
| CIP-008-1 | Incident Reporting and Response Planning |
| CIP-009-1 | Recovery Plans for Critical Cyberassets |

Critical Asset: Facilities, systems, and equipment that, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the electric grid, or would cause significant risk to public health and safety.

Critical Cyberassets: Cyberassets essential to the reliable operation of critical assets.

Cyberassets: Programmable electronic devices and communications networks, including hardware, software, and data associated with bulk electric system assets.

Cybersecurity Incident: Any malicious act or suspicious event that:

- Compromises, or was an attempt to compromise, the electronic or physical security perimeter of a critical cyberasset.
- Disrupts, or was an attempt to disrupt, the operation of a critical cyberasset.

Electronic Security Perimeter: The logical border surrounding a network to which critical cyberassets are connected and for which access is controlled.

There are obvious business advantages to connecting the utility corporate network to the substation, such as access to real-time data, the ability to troubleshoot and remedy problems remotely, and the integration of physical security measures, such as access control and video surveillance. However, these benefits come at the cost of potentially exposing critical cyberassets to these same corporate users.

Some of the cyberdangers include spoofing, denial of service (DoS), replay attacks, viruses, and worms. To address these dangers, the corporate network must be treated as an untrusted network.

Segregating an intersubstation Ethernet network into multiple IP subnets is one approach to meeting the goal of a secure network. Applying the substation boundary, electronic entry point as the demarcation point for different IP subnets may be the only practical choice in many instances because of the reliance on existing utility network infrastructures. Using this method, the substation boundary then aligns cleanly with the electronic security perimeter boundary, as described in the CIP requirements.

Protection against threats from the untrusted corporate network can be handled with a cybersecurity router appliance containing a firewall, VPN access, and IDS. Fortunately, switches and substation-grade routers meeting IEC 61850-3 and IEEE 1613 exist today.

Firewall, VPN, and virtual LANs (VLANs), when used appropriately, provide secure access to different cyberassets within the substation from different groups within the utility. For example, VLANs can be used on the substation LAN to separate protection and control IEDs from remote terminal units (RTUs) and video surveillance equipment. The firewall and/or VPN can then restrict access to those VLANs to individuals from the engineering, SCADA, and operations groups, respectively.

Additional details and examples using VLAN and VPN technology for security can be found in [8] [9] [10].

### *A. Security Using VLANs*

In a utility communications network, security is defined as the immunity of critical traffic to threats. One of the techniques used in providing security from eavesdroppers and hackers is VLANs.

A common definition of a VLAN is a logical group of network nodes that share similar resources and reside in a common broadcast domain, without any router hops. The network nodes do not have to reside in the same physical location but can be spread out across the various facilities of the organization.

In a substation Ethernet network with VLANs, traffic in one substation LAN will share a common signal path in a network with other substation LANs but will not be transported to the IEDs in the other VLANs.

VLANs can be implemented in a number of different ways. Here are some common VLAN types:

- 802.1Q-based VLANs are formed by using 802.1Q tags. The IEEE 802.1Q standard specifies a 4-byte "tag" field that is added after the Ethernet frame's source address. In this document, VLANs with 802.1Q tags are referred to as QVLANs.

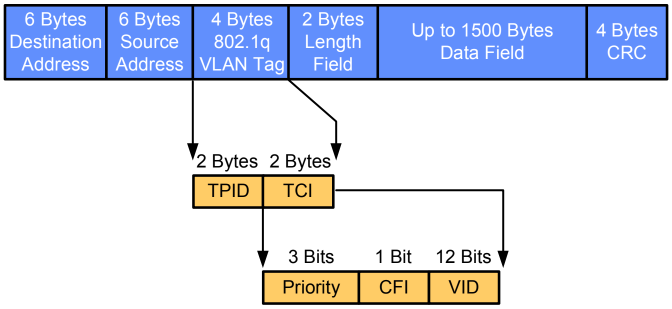


Fig. 6. Ethernet Frame With 802.1Q VLAN Tag

The VLAN tag field consists of the tag protocol identifier field (TPID) – 2 bytes and the tag control information (TIF) – 2 bytes.

The TIF consists of the VLAN ID (12 bits), user priority field (3 bits), and a canonical format indicator (CFI) bit (used for token-ring networks).

- Port-based VLANs (PVLANs) are created by assigning a port to a particular VLAN number. One of the benefits of PVLANs is that they are easy to set up; however, one of the drawbacks is that a user who is physically connected to one port and moving to a different port will require reconfiguration. One of the common applications of PVLANs is to segregate different types of traffic by assigning each type of traffic a separate VLAN. Fig. 7 shows an example of PVLANs.

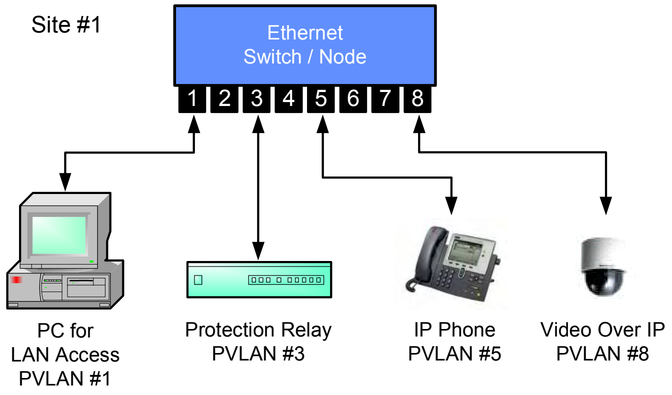


Fig. 7. PVLAN Implementation

- Media access control (MAC) address-based VLANs are created by assigning specific MAC addresses to a particular VLAN.

As integration in the substation takes place, with a goal to reduce the number of devices, it would be useful if a device like a protection relay would be able to classify its different services into QVLANs.

As an example, Fig. 8 shows three sites. Each site has an Ethernet switch/node with a protection relay and a RTU. It is desired to support four different services on each protection relay with each service assigned to a separate QVLAN, as shown in Table VI.

TABLE VI
SERVICES-QVLAN TAG ASSIGNMENT

| Service | QVLAN # |
|---|---|
| Intersubstation GOOSE Messages | 4 |
| Configuration | 5 |
| Intrasubstation GOOSE Messages | 6 |
| Monitoring | 7 |
| RTU | 8 |

The broadcast domain for each service is separate from the other services. However, as the aforementioned advantages are better understood and appreciated by the end users and vendors, it is expected that new products will provide this capability.

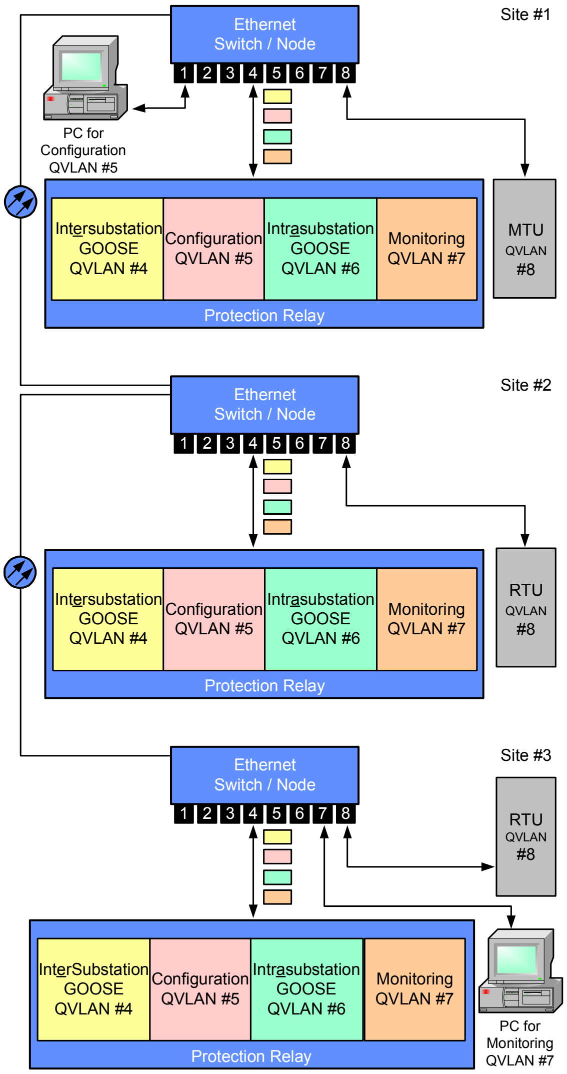


Fig. 8. QVLAN Implementation

### B. *Recommended Engineering Practices for Security Using VLANs*

The recommended engineering practices for security using VLANs are as follows:

- Assign critical traffic to its own VLAN.
- Force "untrusted" source ingressing traffic to a separate VLAN.

### C. *Ethernet Methods for Dependability (Excessive Latency Mitigation)—Quality of Service*

One key consideration in the design of a utility communications network is network dependability. Dependable is defined as the on-time delivery of mission-critical traffic. Thus one of the important network design parameters is the latency for on-time delivery.

In a Synchronous Optical Network (SONET), the latency is deterministic and comprises the following:

- Latency (0 to 125 microseconds) caused by the 8 kilohertz fundamental sampling rate.
- Latency (about 25 microseconds) passing through each repeater node.

- Latency of about 5 microseconds per kilometer for the internode fiber cables.

In an Ethernet network, the latency of a frame comprises the following:

- Propagation delay through the medium.
- Delays in the queue buffers at each network egress port. The time to egress a maximum length frame is 120 microseconds at 100 megabits per second and 12 microseconds at 1 gigabit per second.

Because the Ethernet applications in a utility communications network are diverse and can range from time-sensitive applications (e.g., intersubstation GOOSE messages for teleprotection) to less time-sensitive applications (e.g., download of engineering drawings from the engineering server), the user needs to be able to control traffic classification to achieve quality of service (QoS). Traffic classification is a function of the number of queues in the Ethernet switch/node and the flexibility provided to the user in directing traffic to the queues.

As an example, consider the following intersubstation traffic.

TABLE VII
ETHERNET TRAFFIC CLASSIFICATION

| Traffic Type | Traffic Priority |
|---|---|
| Intersubstation GOOSE Message | 7 |
| Synchrophasor Traffic | 6 |
| Engineering Server Access | 4 |
| Email | 2 |

If the Ethernet switch/node only supports two queues, then the intersubstation GOOSE message and the synchrophasor traffic would be directed to the high-priority queue, while the engineering server access and email would be directed to the low-priority queue. If frames are queued in the high-priority queue, the latency for the frame to reach its final destination increases. The greater the number of queues supported, the greater the flexibility provided to the user in classifying the traffic.

### *D. Recommended Engineering Practices for Dependability*

The recommended engineering practices for dependability are as follows:

- Untrusted-source traffic shall be forced to a lower-priority level than that used for critical traffic. This prevents a hacker from sending DoS attacks (by overloading queues) to the critical-resource IEDs.
- On network paths carrying the critical traffic, the calculated latency shall be acceptable.
  Example: For “five-nines” reliability (the telecom standard), the allowed latency shall be met more than 99.999% of the time.

### *E. American Electric Power Transmission Ethernet*

The following diagram shows the network design implemented for American Electric Power (AEP) transmission substations. This design incorporates many of the choices described previously. Often line positions will have A and B protection. In these installations, A and B Ethernet systems are also used. This matches the redundant switch LAN example to provide full protection and control redundancy, as well as the best system availability.

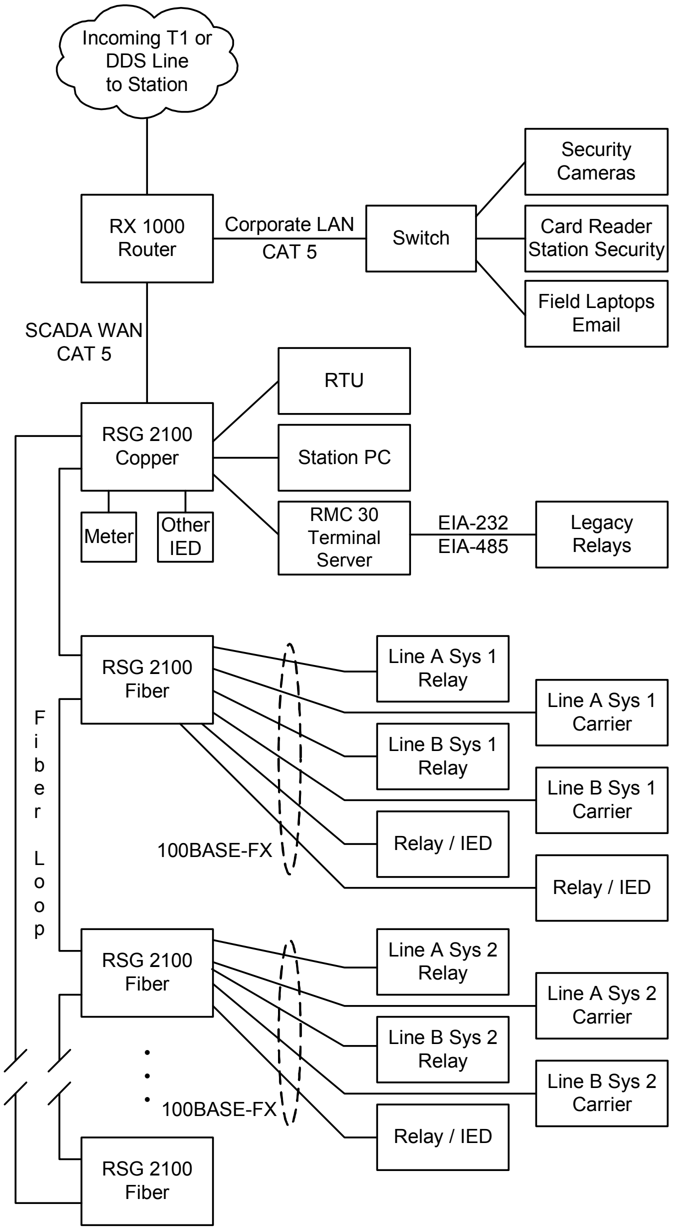


Fig. 9. AEP Ethernet Architecture

Fiber-optic connections are preferred; however, CAT 5 cable is used when cable runs are within the same panel, where ground potential rise is not an issue. Where CAT 5 devices and switches are used, they are kept separate from critical relaying IED connections. For longer runs, fiber-optic cables are preferred, but when CAT 5 is needed, surge protection or media converters and fiber-optic cables are applied.

Several IEDs, relays, and Ethernet switches have the same withstand and immunity capabilities as EIA-232 serial ports, and so they are suitable for this type of connection. Switches and routers that meet the same environmental and withstand requirements as the protective relays are used within the AEP network. Multiple switch systems are connected in a loop configuration with rapid spanning tree protocol to provide quick recovery for cable or switch failures.

Due to product availability, most implemented systems use 10-megabit-per-second connections. Future designs will apply 100-megabits-per-second connections as IEDs become available to support a complete 100-megabit-per-second system, requiring new switch and IED hardware.

Security of the network connections into the substation is provided by firewall appliances using RSA SecurID® authentication. No substation-to-substation communications are allowed. Authenticated corporate connections are allowed, but not back to corporate.

## V. Conclusions

Between the years 2000 and 2007, technological advancements have improved the feasibility of applying Ethernet networks in electrical substations.

1. Standards and products exist for implementation of substation-grade Ethernet networking in substation harsh electrical conditions, proving much higher reliability than commercial and most industrial components.
2. 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. 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.
4. VLANs offer a preferred method for simplifying substation wiring, reducing installation cost, and enhancing the overall security of contemporary high-speed Ethernet communications networks. VPNs offer a method for ensuring privacy and data separation from a substation to its end destination over an untrusted network. When applied properly, VLANs and VPNs offer a powerful new tool in the development of new and existing communications architectures.
5. Ethernet networks are not deterministic; however, by using traffic classification techniques the latency through the network can be managed, thus ensuring the on-time delivery of mission-critical traffic.
6. This paper looks at the LAN technologies necessary to deploy a viable substation LAN and techniques that may be used to improve the overall security and dependability of the Ethernet network.
7. While it may not be necessary for power engineers to get involved in every step of the communications network design process, a clear understanding of the principles and the ability to communicate power system requirements to the IT and communications system professionals is becoming essential for success of the new Ethernet network-based technology.

## VI. References

[1] G. W. Scheer and D. J. Dolezilek, “Comparing the Reliability of Ethernet Network Topologies in Substation Control and Monitoring Networks,” proceedings of the 2nd Annual Western Power Delivery and Automation Conference, Spokane, WA, April 2000. Available: http://www.selinc.com/techpprs.htm

[2] G. W. Scheer and D. J. Dolezilek, “Selecting, Designing, and Installing Modern Data Networks in Electrical Substations,” proceedings of the 9th Annual Western Power Delivery and Automation Conference, Spokane, WA, April 2007. Available: http://www.selinc.com/techpprs.htm

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

[4] IEC 61850-3: Communications Networks and Systems in Substations, Part 3: General Requirements, Section 5: Environmental Conditions, First Edition, 2002-01

[5] G. W. Scheer, “Answering Substation Automation Questions Through Fault Tree Analysis,” proceedings of the 4th Annual Texas A&M Substation Automation Conference, College Station, TX, April 1998. Available: http://www.selinc.com/techpprs.htm

[6] 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.

[7] G. W. Scheer, “Comparison of Fiber-Optic Star and Ring Topologies for Electric Power Substation Communications,” proceedings of the 1st Annual Western Power Delivery and Automation Conference, Spokane, WA, April 1999. Available: http://www.selinc.com/techpprs.htm

[8] V. Skendzic and R. Moore, “Extending the Substation LAN Beyond Substation Boundaries: Current Capabilities and Potential New Protection Applications of Wide-Area Ethernet,” proceedings of the 8th Annual Western Power Delivery and Automation Conference, Spokane, WA, March 2007. Available: http://www.selinc.com/techpprs.htm

[9] G. Leischner and C. Tews, “Security Through VLAN Segmentation: Isolating and Securing Critical Assets Without Loss of Usability,” proceedings of the 9th Annual Western Power Delivery and Automation Conference, Spokane, WA, April 2007. Available: http://www.selinc.com/techpprs.htm

[10] “Virtual LAN Security Best Practices,” VLAN Security White Paper, Available: <www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml>.

[11] R. Breyer and S. Riley, *Switched, Fast and Gigabit Ethernet - Understanding, Building and Managing High-Performance Ethernet Networks,* 3rd ed., Sams, 1998-12-30.

## VII. Additional Reading

L. Anderson, K. Brand, C. Brunner, and W. Wimmer, “Reliability Investigations for SA Communication Architectures Based on IEC 61850,” presented at IEEE St. Petersburg PowerTech, St. Petersburg, Russia, June 2005. Available: http://library.abb.com/GLOBAL/SCOT/scot221.nsf/VerityDisplay/39FFAD3280CF3562C12570D1004DFBCC/$File/IEEE_PetersburgPT05_Paper-604_Andersson-Brand-Brunner-Wimmer.pdf

## VIII. Biographies

**Shawn Coppel** graduated Magna Cum Laude from DeVry Institute of Technology in 1996 with a BS in Electronics Engineering Technology. Shawn is an engineering technologist for American Electric Power in the transmission protection, measurement, and asset engineering section. He specializes in substation communications, phasor measurement, and GPS clock-synchronization technologies. Shawn also spent several years working in telecommunications prototype product development at Lucent Technologies. He served in the U.S. Army during Operation Desert Storm and graduated at the top of his class in radio communications, maintenance, and repair.

**Timothy Tibbals** received his BS in Electronics Engineering from Gonzaga University in 1989. After graduation, he joined Schweitzer Engineering Laboratories, Inc. (SEL) as an application engineer, performing system studies and relay testing. He has also worked as a development engineer and has been part of the development team for many of the communications features and functions of SEL products. He subsequently worked as an application engineer for protection and integration and automation products, assisting customers through product training, seminars, and phone support. He served as the automation services supervisor in SEL's Systems and Services Division for several years before returning to the R&D Division, where he presently serves as the product engineer for the automation and communications engineering products.

**Adrian Silgardo** is a senior product engineer with Schweitzer Engineering Laboratories, Inc. (SEL) in Canada. Adrian has over 13 years experience in the design and implementation of utility communications networks in North American and international markets. Prior to joining SEL, Adrian worked with GE Multilin Canada and Nortel Networks Canada building SONET networks for utilities.

20080221 • TP6317-01