Comparing the Reliability of Ethernet Network Topologies in Substation Control and Monitoring Networks

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

Presented at
UTC Telecom 2002
Las Vegas, Nevada
June 23–26, 2002

Originally presented at the
2nd Annual Western Power Delivery Automation Conference, April 2000

COMPARING THE RELIABILITY OF ETHERNET NETWORK TOPOLOGIES IN SUBSTATION CONTROL AND MONITORING NETWORKS

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

INTRODUCTION

Electric utilities have deployed Ethernet networks in some substations. It appears that soon, more electric power substation networks will incorporate Ethernet. Many Ethernet devices, software, tools, and experts exist as a result of the Internet and of Ethernet local area networks (LANs) in offices and factories. Electric utilities, Electric Power Research Institute (EPRI), and equipment manufacturers are working together to define and deploy the Utility Communications Architecture (UCA). Formal standardization of the UCA is in progress. Intelligent Electronic Device (IED) Manufacturers are providing more equipment that connects to an Ethernet.

This paper contrasts the reliability of substation connection Ethernet topologies to connect devices. Networks based on these topologies are applied to meet the instrumentation and control (I&C) demands of an example substation.

Reliability is one criterion to compare Ethernet systems; other comparative criteria include:

- cost of equipment, installation, and commissioning
- effective data transfer rates
- ease and cost of maintenance
- ease and cost of expansion
- flexibility to use the best IED for each job without undue constraint by network issues
- ease and cost of incorporating existing devices and designs when adding a network to an existing site.

Note that these criteria are not totally independent; for example reliability is a major factor in the cost of maintenance.

ETHERNET BACKGROUND AND COMPONENTS

Network Representation

Often, networks are depicted as a single line, with intersecting short lines connected to each device. Most modern Ethernet networks actually include many more components and connections than are visible in this abstraction. The designer must understand and document all Ethernet components and interconnections to analyze system reliability and to design, procure, install, and maintain the network.

Hubs

A hub is a relatively simple multi-port 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. Ethernet hubs have an average MTBF of 118.9 years.

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. Ethernet switches have an average MTBF of 11.5 years.

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 intra-segment traffic and to route inter-segment traffic to the appropriate destination segment. Ethernet routers have an average MTBF of 9.5 years, but for a price multiplier of 25, they are available with a 35-year MTBF.

IED Ethernet Interfaces

An IED Ethernet interface is an intelligent device which 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. Each device or interface must also use significant processing time to communicate using the interface stacks that are popular today. Many IEDs contain processors with computing capability appropriately matched to their primary purpose. To meet the required performance for high-speed Ethernet connections, the interface usually contains significant processing power. Ethernet interfaces have a typical MTBF of 19.2 years.

Servers

A server collects data from all of the local devices and creates a substation database. Often a local human machine interface graphics package uses data from this database. Servers function at the Application layer of the OSI model. If Ethernet servers are based on industrial personal computers, they have an MTBF of 14.3 years.

Media

Most Ethernet networks employ one of the following media.

- BaseT: specialized copper twisted-pair cable connections
- BaseF: fiber-optic cable.

A data-rate indicator of 10 for 10, or 100 for 100 megabits per second commonly precedes the media designation. Engineers often select fiber-optic cable for substation monitoring and control system communications because it:

- 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
- fewer special tools and skills are required to terminate copper.

Broadcast Data Storms

If the mediation control for data transmission fails, none of the devices on a bus can communicate. An IED communications interface can fail in a mode that corrupts the network. 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.

DEVICE UNAVAILABILITY AND FAULT TREE SUMMARY

An explanation of device unavailability and fault tree construction is included in reference [1]. Reference [2] 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 MTBF. 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 1: Approximate Unavailabilities of Several Components

Component	Unavailability (multiply by 10^{-6})
Substation Communications Processor	30
Ethernet Hub	46

Protective Relay IED Hardware	55
IED Network Interface	285
Equipment Monitoring IED	320
Industrial PC (used as a server)	385
SCADA Gateway	385
Ethernet Switch	477
Ethernet Router	577

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

When you know the unavailability for each component of a system, fault trees are useful to predict the overall system unavailability. Use OR gates to sum the unavailabilities when failure of any of the devices causes a system failure, and AND gates to calculate the product of unavailabilities when all of the failures must occur for the system to fail.

TOPOLOGY COMPARISONS FOR DATA ACQUISITION AND CONTROL

Introduction

The following analyses are based on an actual 138/69 kV substation, with 29 circuit breakers. Full primary and backup protective relays were included in the substation upgrade, for a total of 84 protective relays. For these examples, each relay is equipped with an Ethernet interface. Two communications processors are included as EIA-232 serial-to-Ethernet gateways, for 23 equipment-monitoring devices that are not available with Ethernet capability. A server based on an industrial computer is included to provide HMI and other data clients. A router provides a connection between the substation LAN and a system wide area network (WAN).

The availability analyses focus on the differences between the systems. References [1] and [3] 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 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 in part because it is difficult to quantify software failure rates.

The following five sections summarize the analysis for each of five LANs.

Shared Hub LAN

An Ethernet substation LAN using shared hubs is shown in Figure 1. The boxes without text are IEDs. Boxes marked “GW” are gateways to the equipment monitoring IEDs.

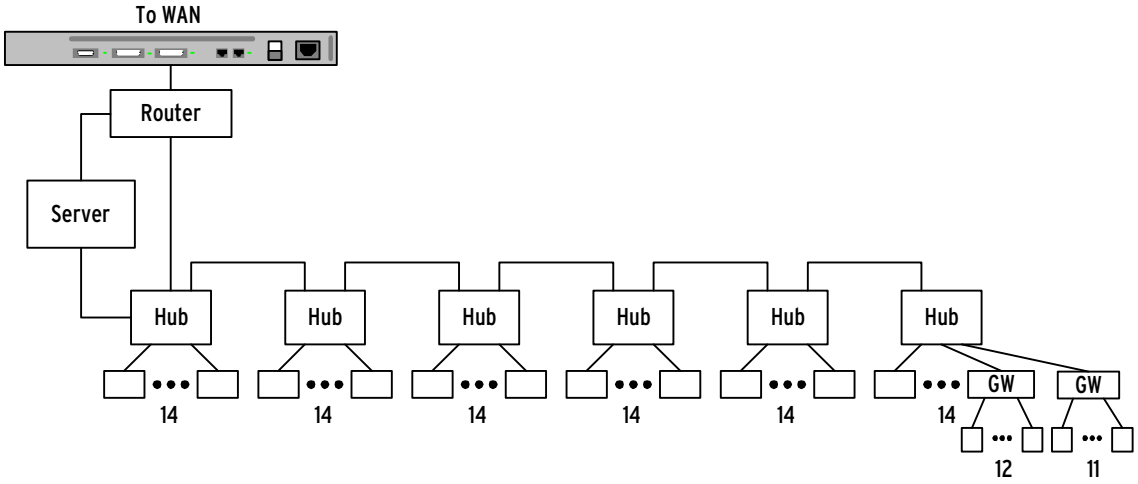

Figure 1: Shared Hub LAN Block Diagram

The fault tree shown in Figure 2 depicts the system unavailability analysis. The top event of the tree indicates that the computed unavailability is the probability that a client accessing either the server or the WAN would not be able to retrieve all of the line data, or would be prevented from controlling any breaker.

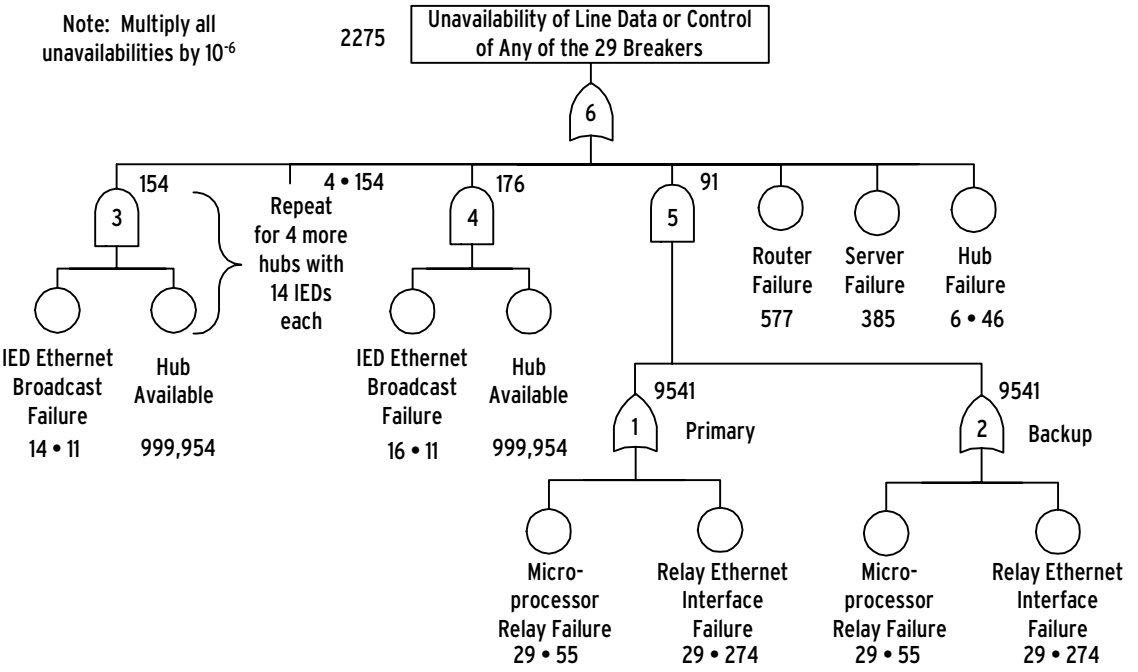

Figure 2: Shared Hub Fault Tree

The system includes primary and backup relay systems. The devices in both the primary and backup systems would have to fail in the same time period to prevent control or monitoring of a breaker, so their system unavailabilities are combined with an AND gate (Gate 5).

This system uses simple shared hubs, so any Ethernet device can cause a broadcast data storm that inhibits the entire network. To allow separation between the failures that impact one device and the broadcast failure that impacts the network, it is appropriate to treat the IED Ethernet interface

unavailability as two failures: 1) the non broadcast mode failures with an unavailability of 274 • 10^{-6}, and 2) the unavailability associated with broadcasts impacting the network, 11 • 10^{-6}, for the total device unavailability of 285 • 10^{-6}.

Starting with the inputs to Gate 1 of the fault tree, there are 29 primary microprocessor relays, with a combined unavailability of (29)(55 • 10^{-6}) = 1595 • 10^{-6}. There are 29 Ethernet interfaces, with a combined non-broadcast failure unavailability of (29)(274 • 10^{-6}) = 7946 • 10^{-6}. The combined unavailability of the primary relays and their interfaces is the sum of these inputs, or 9541 • 10^{-6}.

The backup protection system is identical to the primary system, so it has an identical unavailability. Because both must fail for the system to be unavailable, they are inputs to an AND gate (Gate 5). The predicted unavailability of the combined system is the product of their unavailabilities: (9541 • 10^{-6})(9541 • 10^{-6}) = 91 • 10^{-6}.

IED Ethernet interface broadcast failures affect the network if the associated hub is available and functional. Hub availability = 1 - (hub unavailability) or 1 – (46 • 10^{-6}) = 0.999954. There are six hubs with a total of 86 IED network connections. These include the 58 relays in the primary and backup system involved in line monitoring or breaker control, 26 more relays, and the two gateways to the equipment monitoring devices. The system uses 5 hubs with 14 IEDs each (Gate 3) and one hub with 16 IEDs (Gate 4). The combined unavailability due to network broadcast failures is (5)(14)(11 • 10^{-6})(.999954) + (16)(11 • 10^{-6})(.999954) = 946 • 10^{-6}.

Any one of the following events in Table 2 causes the top event, so their unavailabilities are summed into the top OR gate (Gate 6).

Table 2: Shared Hub Fault Tree Analyses

Cause of Top Event	Unavailability (multiply by 10^{-6})
Primary and Backup Protection Systems Fail	91
Broadcast Data Storm	946
One of Six Hubs Fails: (6)(46 • 10^{-6})	276
Router Fails	577
Server Fails	385
Combined Predicted Unavailability	**2275**
Availability of Top Event: 1 – (2275 • 10^{-6})	**99.7725 %**

Switched LAN

An Ethernet substation LAN using switches has a block diagram similar to Figure 1, except all of the hubs are replaced with switches. The fault tree for the switch-based system is shown in Figure 3, and has fewer gates than the shared hub system. This is because broadcast data storms are stopped by the switch, and impact only the failed Ethernet interface. In this analysis, each Ethernet interface has an unavailability of 285 • 10^{-6}. The combined unavailability of the Switched LAN system is 3921 • 10^{-6}. The availability is 1 - 3921 • 10^{-6} = 99.6079 %.

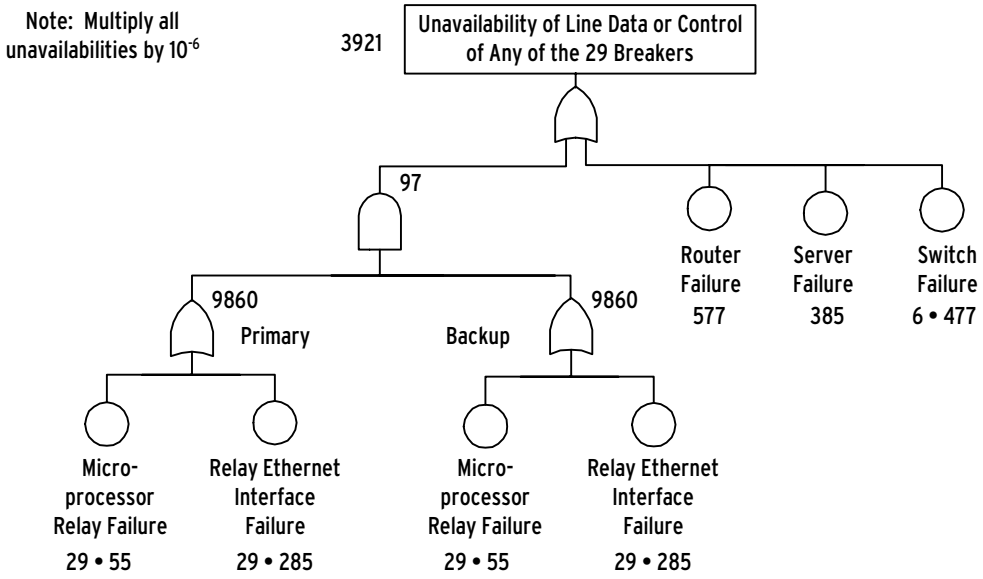

Figure 3: Switch Fault Tree

Redundant Shared Hub LAN

One way to increase availability is to provide redundant networks. Then, instead of a single failure causing the top event, two failures must occur to cause the entire system to fail. The block diagram of a Redundant Shared Hub LAN is shown in Figure 4. The corresponding fault tree is shown in Figure 5. For the primary or backup protection system, the combined unavailability is the sum of the 29 primary relay unavailabilities, and the non-broadcast data storm failures of any of their 29 interfaces $(29)(55 + 274) \cdot 10^{-6}$. For the network, each of the primary and backup systems are subject to the failure of any of the 6 hubs, and the broadcast data storm failure of any of the 86 devices. The primary and backup networks each have an unavailability of $12.22 \cdot 10^{-6}$. The combined unavailability is $1055 \cdot 10^{-6}$. The availability is 99.8945 %, considerably more than either the Shared Hub or Switched LAN topologies.

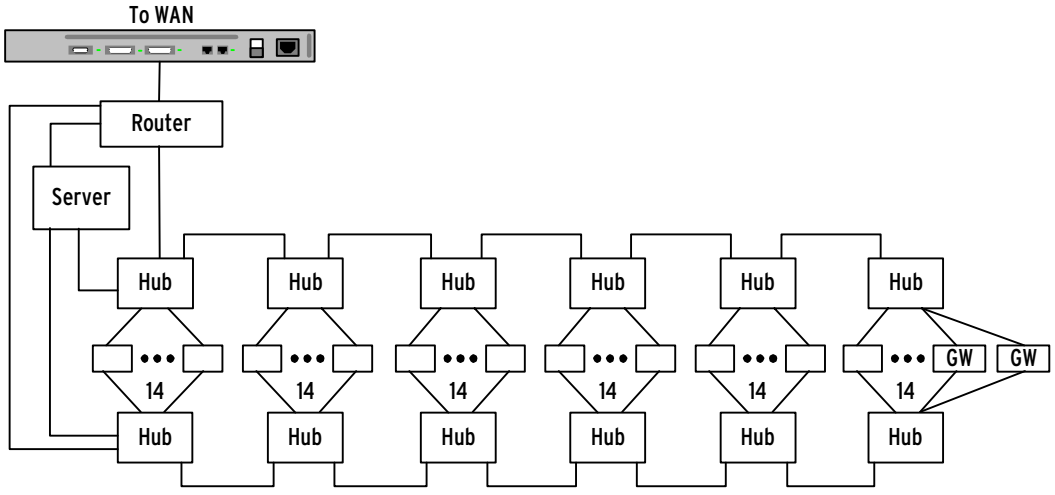

Figure 4: Redundant Shared Hub Block Diagram

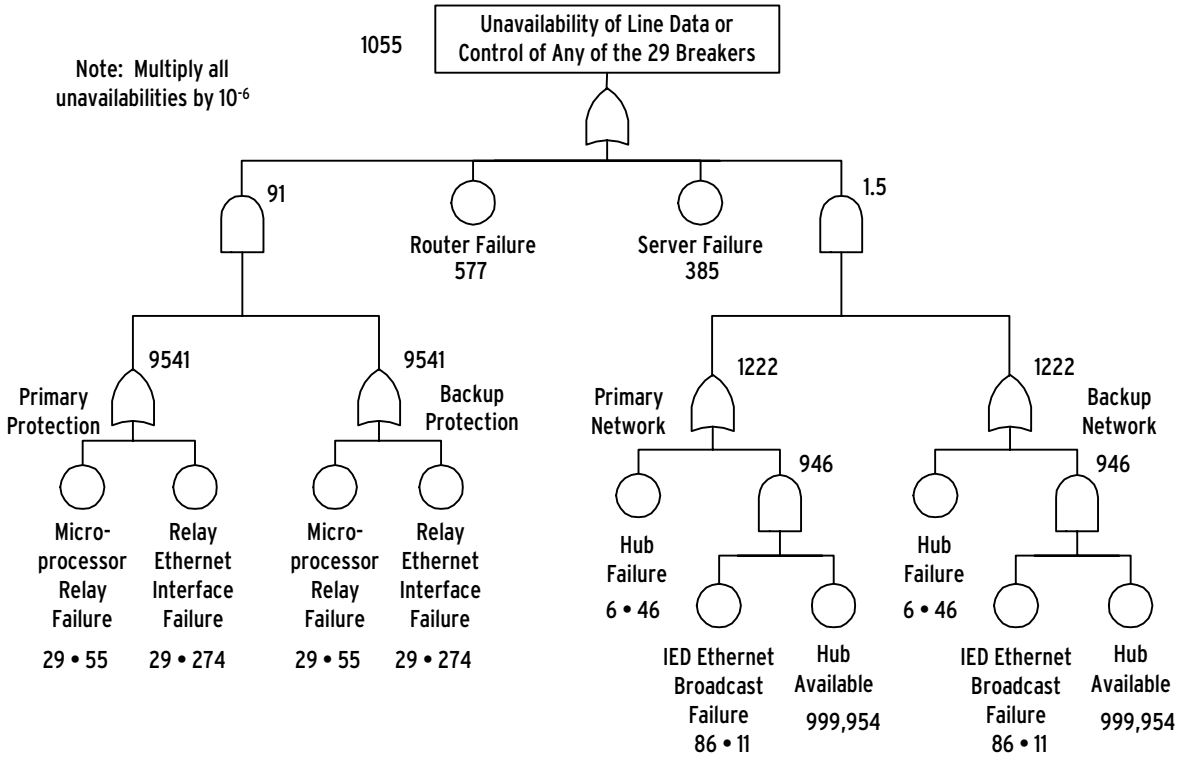

Figure 5: Redundant Shared Hub Fault Tree

Redundant Switched LAN

The block diagram for a substation with redundant switched LANs is similar to Figure 4, except all of the hubs are replaced with switches. In this analysis, each Ethernet interface has an unavailability of $285 \cdot 10^{-6}$. The combined unavailability of the primary and backup protection is $97 \cdot 10^{-6}$, as in the non-redundant switched case. The primary and backup networks each have six switches, $(6 \cdot 477 \cdot 10^{-6})$. The combined network unavailability is $(2862 \cdot 10^{-6})^2$, or $8.19 \cdot 10^{-6}$. The overall unavailability of the Redundant Switched LAN is $1067 \cdot 10^{-6}$, the sum of the protection network, server, and router unavailabilities. The availability is 99.8932 %, slightly less than the Redundant Shared Hub LAN topology.

Redundant Servers, Routers, and Switches LAN

Rather than replicating the entire network, a designer can split the communications network into primary and backup networks, connected to their respective primary and backup protection systems. Figure 6 depicts fully redundant protection and communications systems. The only non-redundant components are in the equipment monitoring subsystem. The fault tree for this system is shown in Figure 7. The primary and backup systems each have an unavailability of $12{,}253 \cdot 10^{-6}$. The combined system unavailability is $150 \cdot 10^{-6}$. The availability is 99.9850 %.

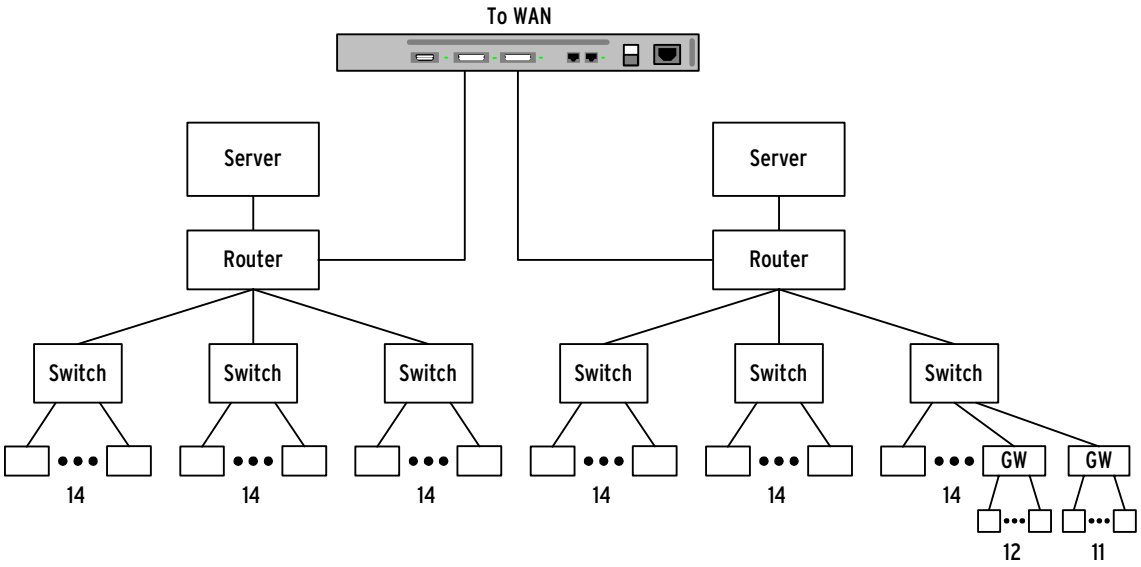

Figure 6: Redundant Servers, Routers, and Switches LAN Block Diagram

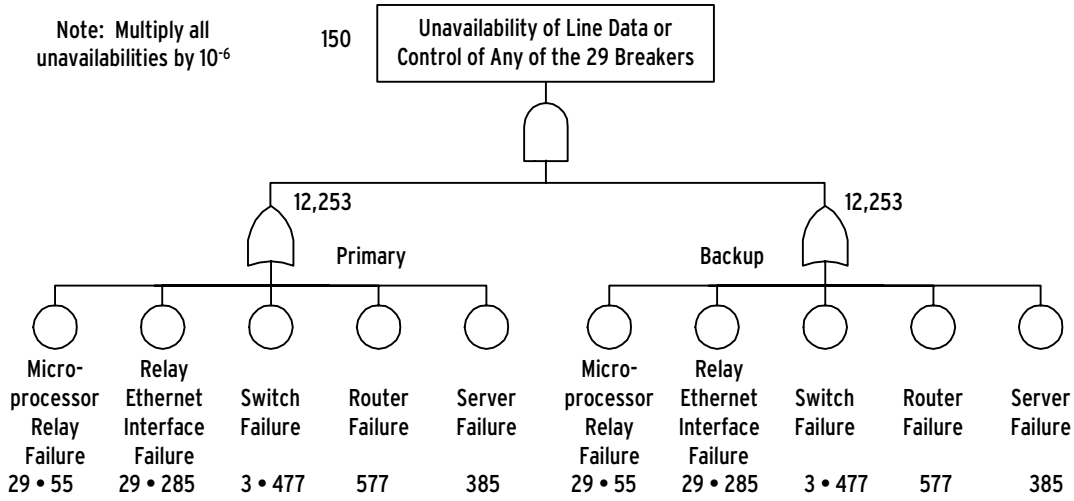

Figure 7: Redundant Servers, Routers, and Switches Fault Tree

Availability Comparison

Table 3 summarizes the connection topology availabilities discussed. The predicted annual hours out of service is the unavailability times the number of hours in a year.

Table 3: Availabilities of Systems to Retrieve all Line Data and Operate Any Breaker

Ethernet LAN	Availability %	Predicted Annual Hours Out of Service
Switches	99.6079	34.3
Shared Hubs	99.7725	19.9
Redundant Switches	99.8932	9.3
Redundant Shared Hubs	99.8945	9.2
Redundant Servers, Routers, Switches	99.9850	1.3

The susceptibility of shared hubs to data storms might lead you to suspect that a hub-based system would have a worse availability than a switched system. However, in the examples, the hub-based system is more available, due to the longer MTBF of the simple hub compared to the more complex switch. The redundant hub and switch systems are representative of actual installations, and exhibit better availabilities than the respective non-redundant systems. The fully separate system with redundant servers, routers, and switches exhibits the best availability of all these systems.

Cost Comparison

Costs are provided in this section, to aid in identifying the cost and availability trade-offs for the LANs. Table 4 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 maintenance costs are summarized in the last column of Table 4, and include labor and non-warranty material costs for all of the predicted equipment failures in ten years.

Table 4: Typical Equipment and Maintenance Costs of Ethernet LANs

Ethernet LAN	Initial Equipment Cost ($)	Ten-Year Maintenance Cost ($)
Redundant Switches	156,000	173,000
Switches	123,000	147,000
Redundant Shared Hubs	121,000	129,000
Redundant Servers, Routers, Switches	116,000	156,000
Shared Hubs	106,000	127,000

SENSITIVITY TO LOW MTBF OF AVAILABLE NETWORK DEVICES

The above comparisons calculate unavailability using MTBF averages for devices manufactured and deployed today. Increased applications of Ethernet in industrial and electric utility applications may create demand for Ethernet devices that are designed for longer Mean Times Before Failure. If unavailabilities comparable to protective relays are obtained for interfaces and switches, then we can contrast the same topologies using an unavailability of $55 \cdot 10^{-6}$ instead of the values in Table 1. If these theoretical hubs, switches, and routers existed, the predicted availabilities of networks that use them would be the values summarized in Table 5. The systems are shown in ascending order of availability.

Table 5: Availabilities of Systems Using Future High MTBF Components to Retrieve All Line Data and Operate Any Breaker

Ethernet LAN With Theoretical High MTBF Devices	Availability %	Predicted Annual Hours Out of Service
Shared Hubs	99.8330	14.6
Switches	99.9220	6.84
Redundant Shared Hub	99.9550	3.93
Redundant Switches	99.9550	3.94
Redundant Servers, Routers, Switches	99.9986	0.126

ANALYSES WITH OTHER TOP EVENTS

The analyses above focus on availability of the systems to retrieve all line data and operate all breakers. This top event corresponds to the system availability view that is often applied to SCADA master systems.

Analyses using other top events reveal different facets of the system availability. For example, a top event of "Unable to Control Breaker Number 7 or Retrieve Line Data from Line 7" would have only the impacts of the system on communications with a specific relay. Analysis on this basis will yield a better availability for independent topologies than for shared topologies.

TOPOLOGY COMPARISONS FOR RELAY-TO-RELAY COMMUNICATIONS

Another top event is "Unable to Communicate Relay-to-Relay Protection Data." Use this top event to compare using an Ethernet link to using direct links for relay-to-relay communications. Consider only the components and connections that impact the communications path between two relays in different segments of each Ethernet LAN previously analyzed.

For the Shared Hub LAN, the primary and backup protection systems each include the two relays, and their Ethernet interfaces. The non-broadcast failures of the interfaces and the relays yield an unavailability of $658 \cdot 10^{-6}$ for the primary or backup protection. The combined unavailability is $0.433 \cdot 10^{-6}$. Add the unavailabilities of 6 hubs and 86 broadcast failures for a system unavailability of $1222 \cdot 10^{-6}$. The availability is 99.8778 %.

For the Switched LAN, the primary and backup protection systems each include the two relays, and their Ethernet interfaces, for an unavailability of $680 \cdot 10^{-6}$. The combined unavailability is $0.462 \cdot 10^{-6}$. Add the unavailabilities of 6 switches for a system unavailability of $2862 \cdot 10^{-6}$. The availability is 99.7138 %.

For the Redundant Hub LAN, the items impacting the peer-to-peer availability in the primary or backup protection systems are two relays ($2 \cdot 55 \cdot 10^{-6}$) and the non-broadcast failures of their Ethernet interfaces ($2 \cdot 273 \cdot 10^{-6}$). The combined unavailability of the protection systems is $0.430 \cdot 10^{-6}$. The primary and backup networks each have 6 hubs ($6 \cdot 46 \cdot 10^{-6}$) and broadcast failures for 86 IEDs ($.9999 \cdot 86 \cdot 11 \cdot 10^{-6}$), for an unavailability of $1222 \cdot 10^{-6}$. The combined primary and backup network unavailability is $1.49 \cdot 10^{-6}$. The total combined unavailability is $1.92 \cdot 10^{-6}$. The availability is 99.9998 %.

For the Redundant Switched LAN, the primary and backup systems each include the two relays ($2 \cdot 55 \cdot 10^{-6}$) and their Ethernet interfaces ($2 \cdot 285 \cdot 10^{-6}$), for an unavailability of $680 \cdot 10^{-6}$. The combined unavailability is $0.462 \cdot 10^{-6}$. The primary and backup networks each have 6 switches ($6 \cdot 477 \cdot 10^{-6}$), and a combined unavailability of $8.19 \cdot 10^{-6}$. The total combined unavailability is $8.65 \cdot 10^{-6}$. The availability is 99.9991 %.

For the Redundant Servers, Routers, and Switches LAN, the items impacting the relay-to-relay availability in the primary or backup systems are two relays ($2 \cdot 55 \cdot 10^{-6}$), their Ethernet interfaces ($2 \cdot 285 \cdot 10^{-6}$), two switches ($2 \cdot 477 \cdot 10^{-6}$), and one router ($577 \cdot 10^{-6}$). The primary or backup system has an unavailability of $2211 \cdot 10^{-6}$, for a combined unavailability of $4.89 \cdot 10^{-6}$. The availability is 99.9995 %.

For a direct, relay-to-relay connection, the primary or backup system includes two relays ($2 \cdot 55 \cdot 10^{-6}$) and two dedicated fiber interfaces ($2 \cdot 10 \cdot 10^{-6}$), for a net unavailability of $130 \cdot 10^{-6}$. The combined unavailability of the primary plus backup systems is $0.0169 \cdot 10^{-6}$. The availability is 99.9999 %.

Table 6 summarizes the unavailabilities and availabilities of the networks and direct links for relay-to-relay communications within a substation, arranged in descending order of availability.

Table 6: Relay-to-Relay Communications in a Substation

Network	Availability %	Predicted Annual Hours Out of Service
Switches	99.7138	25
Shared Hubs	99.8778	10.7
Redundant Switches	99.9991	.07
Redundant Servers, Routers, Switches	99.9995	.04
Redundant Shared Hubs	99.9998	.01
Direct	99.9999	.00014

The focus of this paper is on Ethernet applications within substations. See the Appendix for guidelines for station-to-station relay communications analysis.

CONCLUSIONS

Of the five LANs analyzed, the topology with redundant, independent networks, is the most available to operate any breaker and retrieve all power line data. This topology is the second lowest in equipment cost of the five. If this topology becomes broadly accepted for substation automation, it could further reduce the cost and unavailability of IED interfaces, because it does not use the standby-failover feature of the interfaces.

If Ethernet equipment manufacturers provide devices with much better Mean Times To Fail than existing devices, then the same topology with redundant, independent networks will still be the most available for the general I&C cases. The ranking of networks that use switches will surpass the ranking of those with shared hubs. All of the systems using higher MTTF devices are more available than existing systems. If Ethernet is to be used in critical industrial and substation systems, we recommend that IED manufacturers design and supply Ethernet components with higher Mean Times To Fail.

For relay-to-relay communications, direct communications external to the LAN are far more available than any of the LANs. This is due to the number of devices involved in the LAN, and the relative complexity of the devices. If a LAN is used for relay-to-relay protection data, the Redundant Shared Hubs LAN has the best availability.

If Ethernet is used for the station I&C, we recommend the Redundant Servers, Routers, and Switches topology. For relay-to-relay protection communications, we recommend direct fiber connections, separate from the network.

PROCESS SUMMARY

It is important to identify and characterize all of the devices in a network and their interconnections to analyze the reliability of the networks.

To analyze alternatives, obtain the MTBF and MTTR data for each component of the system, calculate unavailabilities, and construct and analyze fault trees for each option under consideration. Use the fault trees to identify areas that can be replicated to reduce their contribution to the system unavailability, and modify the system to reflect the improvement. Calculate the cost, and determine the importance of the remaining evaluation criteria.

Choose top-events for the fault trees that yield the unavailability of the system to accomplish a well-defined task or group of tasks. In this paper we contrast the “Availability to Retrieve all Line Data and Operate Any Breaker” for each system, which is comparable to the availabilities typically considered in SCADA master comparisons. In addition, we contrast the systems’ availabilities to “Communicate Relay-to-Relay Protection Data” within the substation. These top-events directly address Ethernet applications currently discussed in electric power industry meetings.

APPENDIX: GUIDELINES FOR ANALYZING RELIABILITY OF RELAY-TO-RELAY COMMUNICATIONS BETWEEN STATIONS

The focus of this paper is on Ethernet networks applied within substations. Some utility engineers have considered using a WAN to transmit relay-to-relay protection information between substations. This Appendix provides guidelines for calculating the estimated availability of inter-station relay-to-relay communications.

Consider two substations identical to the example station used in the case comparisons. For each of the six cases for relay-to-relay communications within a substation, consider the additional failure modes of inter-station communication. If the two substations both employ a shared hub, redundant shared hub, switched, or redundant switched network, then calculate the unavailability in each substation with the following modifications to the appropriate calculation in the paper:

- Use the unavailability for only one relay and one Ethernet interface in each of the primary and backup protection systems.
- Add the unavailability of the router to the station unavailability.

For the redundant routers, servers and switches system in each substation:

- Use only one relay, one Ethernet interface, and one switch in each of the primary and backup systems.
- Note that the routers are already included in the substation analysis.

The overall predicted unavailability is the sum of two substation network unavailabilities, plus the unavailability of the WAN components, interconnections, and fiber. Analyze the WAN or WANs with a methodology similar to those employed in this paper for each LAN. Outside of the substation, add the unavailability of the fiber-optic cable due to digging errors [2]. At each additional site that impacts the WAN performance, include the power supply source in the unavailability analysis.

For the direct relay-to-relay connection between substations, use a relay and fiber-optic transceiver in the primary and backup system of each substation. Outside of the substation, include the unavailability of the fiber-optic cable due to digging errors [2]. If the fibers are in a common cable or trench, treat the unavailability of the fiber-optic cables as an event common to the primary and backup systems. If separate fiber-optic cables are installed with separated routes, include the fiber-optic cable unavailabilities in each of the primary and backup systems.

REFERENCES

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

[2] 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.

[3] 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.

[4] D. J. Dolezilek, D. A. Klas, "Using Information From Relays to Improve Protection," Proceedings of the 25th Annual Western Protective Relay Conference, Spokane, Washington, October 13-15, 1998.

BIOGRAPHY

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 in the Marketing and Customer Services Division as Market Manager for automation and communications products. 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, NSPE, and the ISA.

David J. Dolezilek received his B.S. in Electrical Engineering from Montana State University in 1987. In addition to independent control system project consulting, he worked for the State of California, Department of Water Resources, and the Montana Power Company before joining Schweitzer Engineering Laboratories, Inc. in 1996 as a system integration project engineer. In 1997 Dolezilek became the Director of Sales for the United States and Canada, then moved on to serve as the Engineering Manager of Research and Development in SEL's Automation and Communications Engineering group. In 2000, Dolezilek was promoted to Automation Technology Manager to research and design automated systems. He continues to research and write technical papers about innovative design and implementation affecting our industry, as well as participate in working groups and technical committees. He is a member of the IEEE, the IEEE Reliability Society, and the International Electrotechnical Commission (IEC) Technical Committee 57 tasked with global standardization of communication networks and systems in substations.