Performance of Redundant Ethernet Networks for Electric Substation Instrumentation and Control

Veselin Skendzic and Gary W. Scheer
Schweitzer Engineering Laboratories, Inc.

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

Originally presented at the
11th Annual Western Power Delivery Automation Conference, April 2009

Performance of Redundant Ethernet Networks for Electric Substation Instrumentation and Control

Veselin Skendzic and Gary W. Scheer, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Electric utility engineers use Ethernet networks in electric power substations for an increasing number of applications, including supervisory control and data acquisition (SCADA), automatic control, protection, remote maintenance, and disturbance analysis. Engineers recognize that many of these functions are mission critical and therefore specify redundant Ethernet networks to increase the availability. An additional drive for redundant Ethernet networks stems from applying the IEC 61850 Process Bus to provide data from instrument transformers to protection and other high-speed control subsystems.**

Equipment suppliers offer devices that have different port connection and failover logic options to support a variety of network topologies with complete redundancy and partial redundancy with hot, warm, and cold standby failover methods. This paper compares several redundant Ethernet network approaches and examines their suitability for the instrumentation and control (I&C) demands of electrical substations. The paper analyzes performance and summarizes reliability and example cost tradeoffs.

This paper provides data, analysis, and methods to aid electric utility engineers and equipment suppliers as they evaluate and design I&C systems using Ethernet networks in electrical substations.

I. Introduction

Electrical substation instrumentation and control (I&C) systems use a variety of topologies, networks, and protocols to communicate between multiple nodes. Typical nodes include the following:

- Intelligent electronic devices (IEDs), such as, protective relays, meters, and dedicated controllers
- Local computers, programmable logic controllers, or programmable automation controllers (PACs), providing data concentration and automatic control
- Local displays or human-machine interfaces (HMIs)
- Wide-area network (WAN) links
  - Supervisory control and data acquisition (SCADA) masters located in control centers
  - Wide-area measurement and control (synchrophasor) systems
  - Remote engineering access and maintenance workstations
  - Event report gathering and analysis systems

While switched Ethernet has emerged as a communications network of choice, network topologies vary widely with no established industry practice [1]. This situation is further complicated by the wide variety of power system applications, ranging from systems internal to industrial facilities up to critical high-voltage (HV) and extra-high-voltage (EHV) transmission systems.

II. Ethernet Networking in Electrical Substations

A. Ethernet Switches

In basic terms, an Ethernet switch detects the addresses of the devices connected to its ports. When the switch receives a packet, it matches the destination address of the packet to the port address list to determine the port to which it should retransmit the packet. In substations, the links between the devices and switches typically operate at a rate of 100 megabits per second. Station networks with a large number of nodes typically use a 1 gigabit-per-second backbone between the switches and routers.

B. Ethernet Link Detection and Link Faults

An Ethernet device determines that it is connected to a device that successfully communicates with it. Successful communication indicates a "linked" status that is often displayed on light-emitting diode (LED) indicators on the devices to aid in solving network problems. Failure to establish a link is designated as a "link fault" or "loss of link." The link fault is reported as an alarm and may be used to initiate failover to an alternate network or network path. If a device does not detect packet receipt, it may be set up to send a far-end fault indication (FEFI) message. Typically, this is employed in full-duplex, fiber-optic connections to notify the remote node that its transmitted data packets are not reaching the destination. To facilitate switching to backup networks, many switches can be configured to fault the links on their downstream ports for link faults detected on upstream ports.

C. Ring and Spanning Tree Switching

When a network topology includes more than one path to a device, the networking devices often need to disable some of the paths. This enables efficient use of the network and avoids endlessly circulating the same message or bombarding the destination device with multiple copies of the identical message that followed different paths [2].

The standard solution is to employ Rapid Spanning Tree Protocol (RSTP), as defined in the IEEE Standard 802.1D-2004 [3]. RSTP 2004 is event driven, with typical failover times of 30 to 60 milliseconds, depending on the ring size. Earlier versions of the standard defined Spanning Tree Protocol with 30- to 50-second switching times and RSTP (1998) with an approximate 1.5-second recovery time.

D. Environment and Reliability Standards

Because substation Ethernet is used to carry critical SCADA and protection traffic, all substation Ethernet network devices must meet the same environmental and reliability standards as the protection system devices defined in IEEE Standard 1613-2003 [4].

III. Performance and Reliability Requirements

A. Performance Requirements

Substation Ethernet networks must carry a wide variety of traffic with differing performance requirements. Those requirements include security, correctness, and message delivery timeliness. Some substation applications use connection-oriented protocols, such as Transmission Control Protocol/Internet Protocol (TCP/IP), which achieve reliable transmission through message repetition and frame acknowledgement (thus resulting in increased latency). Other protocols, such as User Datagram Protocol/Internet Protocol (UDP/IP), provide connectionless service that is more appropriate for time-sensitive applications, such as synchrophasors. Most critical real-time applications use Layer 2 (data link layer) messages specifically optimized for power system protection and control. Layer 2 messages include IEC 61850 Generic Object-Oriented Substation Event (GOOSE) and IEC 61850-9-2 Process Bus messages [5].

Regardless of the message type, virtually all substation applications have strict time delivery requirements that must be met by the Ethernet network. Delivery time requirements are not limited to normal operation but must be met during network failure and recovery events.

In some applications, communications network failures can be mitigated by using local intelligence or conventional protection schemes that are independent of data communication [6]. However, wide-area applications, including SCADA and synchrophasors, require that the communication be restored in a timely manner. This creates the need for communications network redundancy and the development of methods for evaluating redundant network failure modes and recovery.

Table I summarizes typical recovery time requirements for different substation network applications. The requirements are based on data published in [5], with the addition of time synchronization, engineering access, and synchrophasor applications.

TABLE I
NETWORK RECOVERY TIME REQUIREMENTS

Application	Protocol	Application Recovery Time	Network Recovery Time
Time Synchronization (IEEE 1588, SNTP)	UDP Layer 2	Ride through required	<1 s typical
Engineering Access (FTP, Telnet)	TCP/IP	<500 ms	<250 ms
SCADA Scan	TCP/IP	<500 ms	<250 ms
IEEE C37.118 Synchrophasors	TCP/IP UDP/IP	<16 ms	<8 ms
IEC 61850 GOOSE-Based Automation	Layer 2	<20 ms (HV) <100 ms (MV)	<10 ms
IEC 61850 GOOSE-Based Tripping and Protection	Layer 2	<3 ms (HV) <10 ms (MV)	<1.5 ms
IEC 61850 Process Bus	Layer 2	<2 ms no loss of data	<1 ms network latency

The network recovery time column illustrates additional application overhead, which makes it impossible to allocate the entire available time budget to the network recovery process. A detailed analysis based on these requirements is in Section V.

B. Reliability Requirements

1) SCADA

Historically, SCADA systems replaced dispatching personnel to substations to perform switching operations or record measurements. In the early days of SCADA system deployment, the remote terminal units (RTUs) were treated as nonmission-critical components, because if a unit failed, the easy backup was to send a person to the station. Today, the information that SCADA systems exchange with control centers is considered mission critical, providing situational awareness to systems dispatchers and real-time information for fast-acting, real-time control systems. Modern SCADA system specifications often require 99.999 percent availability.

2) Protective Relays, Process Bus, and High-Voltage Equipment Control

Protective relays monitor inputs to detect faults on power lines and apparatus and perform automatic high-speed control actions to disconnect power from the faults.

Process Bus is used to establish connections between protective relays and the primary system equipment. The term applies to the IEC 61850-9-2 Sampled Value (SV) message service originally intended to stream instantaneous measurement values from nonconventional instrument transformers. This service was recently extended to include digitizing any kind of instrument transformer output and is aimed at minimizing substation yard wiring [7].

High-voltage equipment control, such as communications-based tripping, is accomplished by using IEC 61850 GOOSE messages [8]. Both SV and GOOSE messages are absolutely critical for power system operation. Delays in message delivery can lead to protection system misoperation, failure to trip, or inadequate coordination. Redundant systems are mandatory [9].

Practical use of this technology is still limited, with the majority of deployed systems using GOOSE for interrelay communications but relying on conventional wiring for breaker tripping applications. Pilot projects are under way to evaluate overall system performance and develop appropriate installation, testing, and maintenance methods.

Protection and automatic control systems often require availability of at least 99.999 percent.

IV. Topologies

Fig. 1 shows a local-area network (LAN) that connects microprocessor-based protective relays, information processors, local HMI, and other devices, including meters, I/O processors, PACs, and other monitoring and control equipment. We examine eight example topologies of the many possible network configurations.

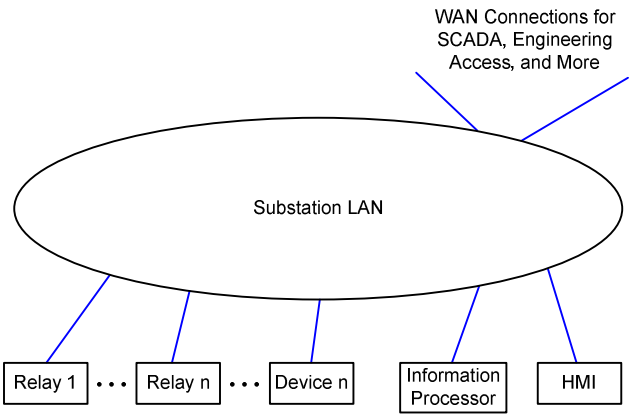

Fig. 1. Generic Substation LAN

A. Single Network

Fig. 2 depicts a single tree network topology with no redundancy. Blocks S1 through S4 indicate Ethernet switches.

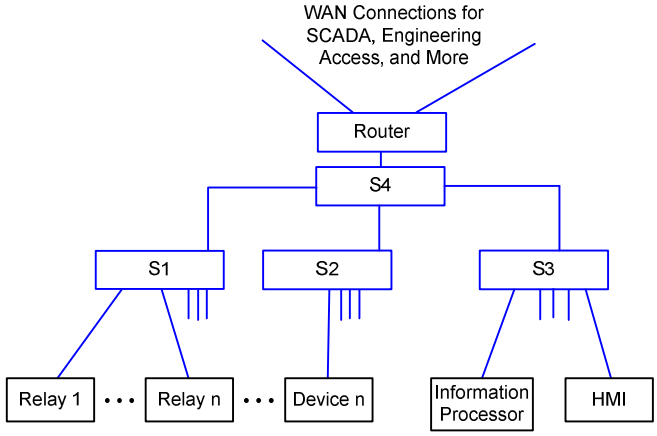

Fig. 2. Single Tree Network Topology Example

B. Single Network With Redundant Paths

Fig. 3 shows a network with a switch ring topology with each switch connected to IEDs via star point-to-point connections. If the path in one direction around the ring is interrupted, the network forwards messages using an alternate path around the ring.

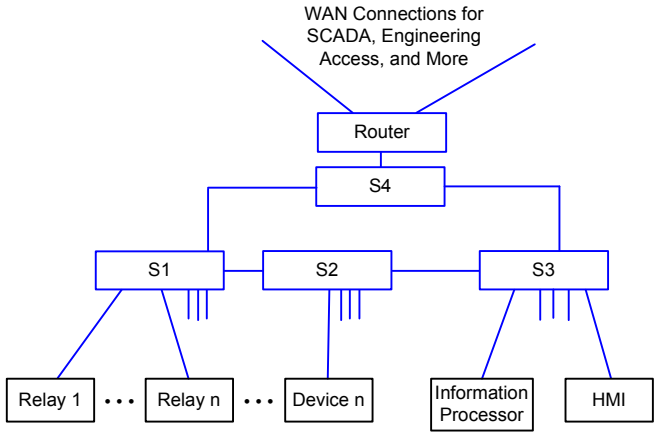

Fig. 3. Single Ring Network Topology Example

C. Dual Networks With Failover

The topology shown in Fig. 4 uses two separate networks. Each device has two Ethernet connections, one for each network. All communications normally go through the primary network. In the event of a primary network failure, each device transfers to the backup network.

D. Dual Redundant-Path Networks With Failover

The topology shown in Fig. 5 uses two separate networks. Each device has two Ethernet connections, one for each network. All communications normally go through a primary network. If the path in one direction around the ring is interrupted (e.g., clockwise), the network transfers to using the other path around the ring (e.g., counterclockwise). In the event of a network failure, each device transfers to the backup network.

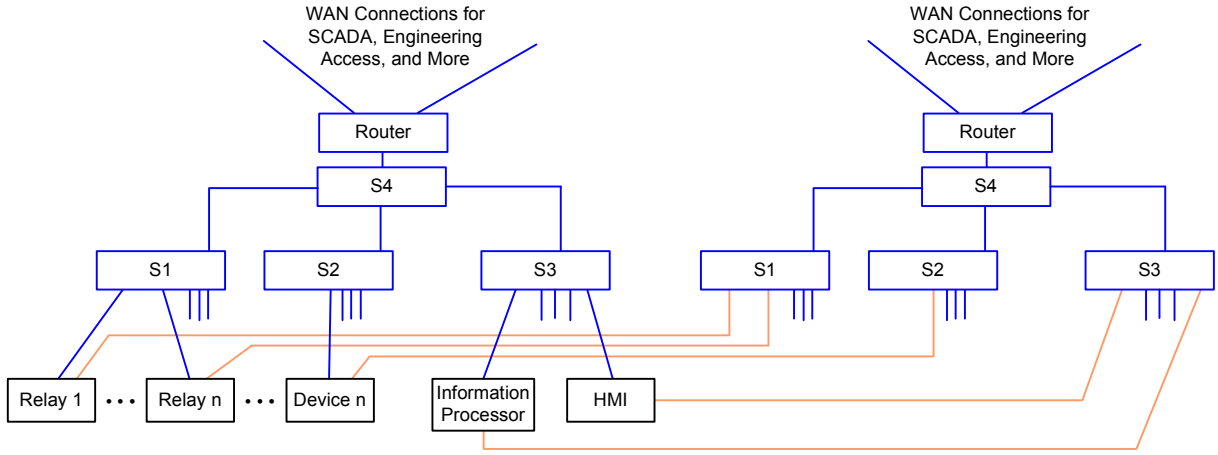

Fig. 4. Dual Networks With Failover

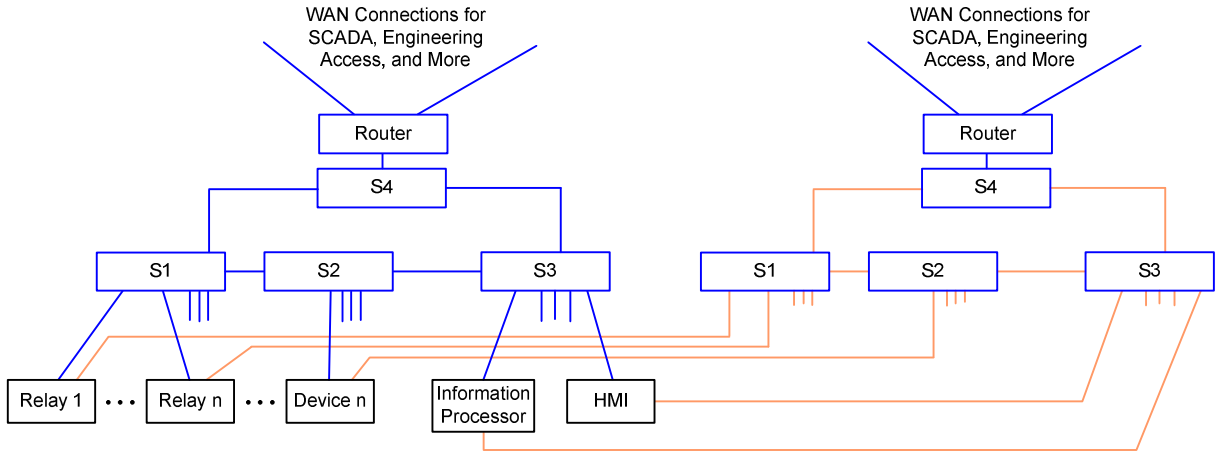

Fig. 5. Dual Redundant-Path Networks With Failover

E. Fully Independent Dual Networks and Redundant Devices

Primary relays are connected to a primary network, and dual-primary relays connect to a dual-primary copy of the network. There is no connection in the station between the networks (Fig. 6).

F. Dual Redundant-Path Networks With Point-to-Point Process Bus Links

This topology is similar to the topology described in Section IV, Subsection D, with the addition of merging units (MU) with a point-to-point connection to each relay (Fig. 7).

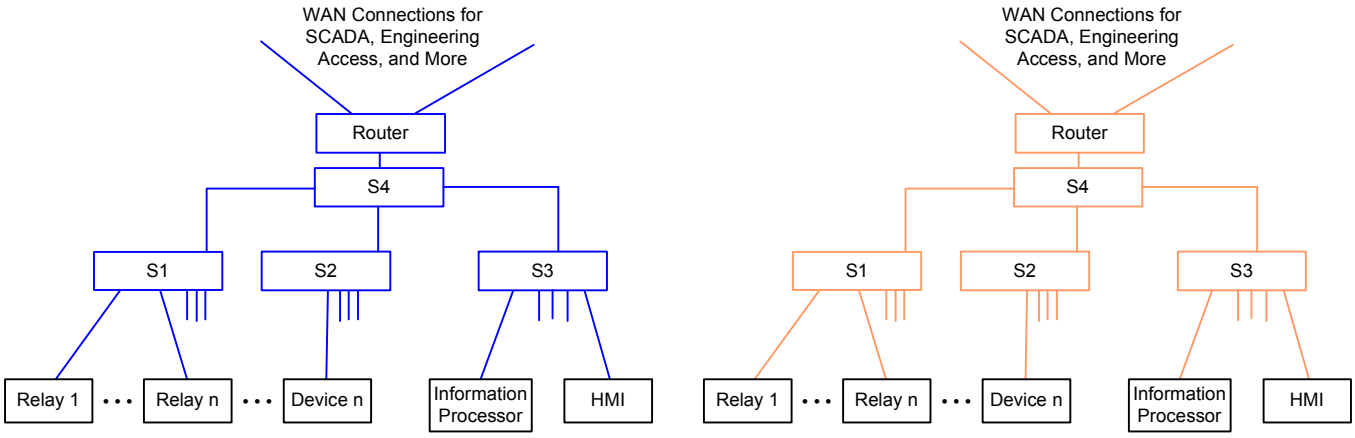

Fig. 6. Fully Independent Dual Networks With Redundant Devices

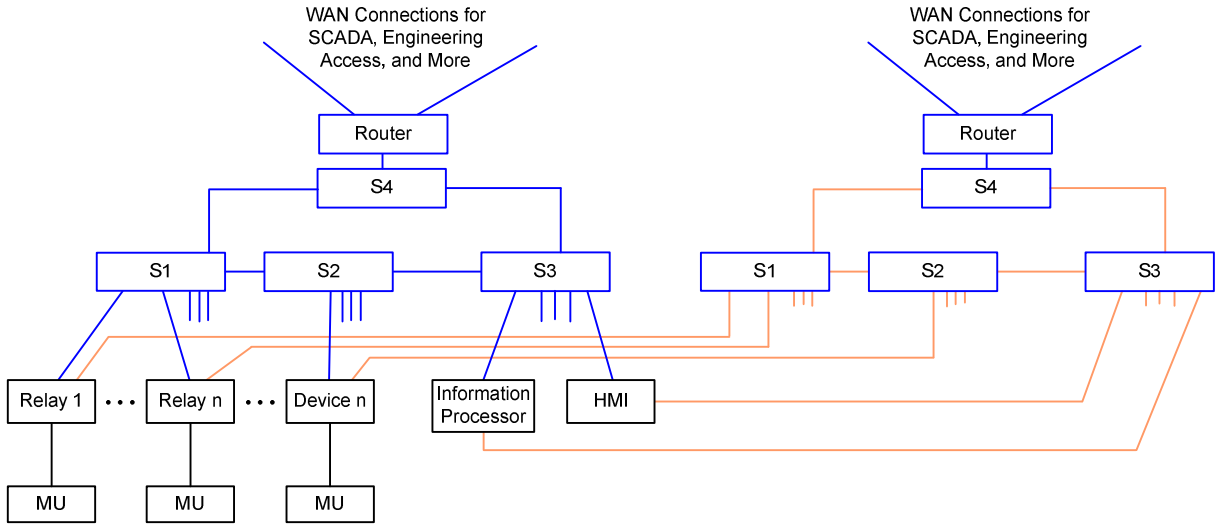

Fig. 7. Dual Redundant-Path Networks With Point-to-Point Process Bus Links

G. Fully Independent Dual Networks With Redundant Devices and Point-to-Point Process Bus Links

Primary relays are connected to a primary network, and primary merging units have point-to-point connections to primary relays. Dual-primary relays are connected to a dual-primary copy of the network, and the dual-primary merging units have point-to-point connections to the relays. There is no connection in the station between the networks (Fig. 8).

H. Fully Independent Dual Networks With Redundant Devices and Network-Based Process Bus

Primary relays and merging units are connected to a primary network, and dual-primary relays and merging units connect to a second network. There is no connection in the station between the networks (Fig. 9).

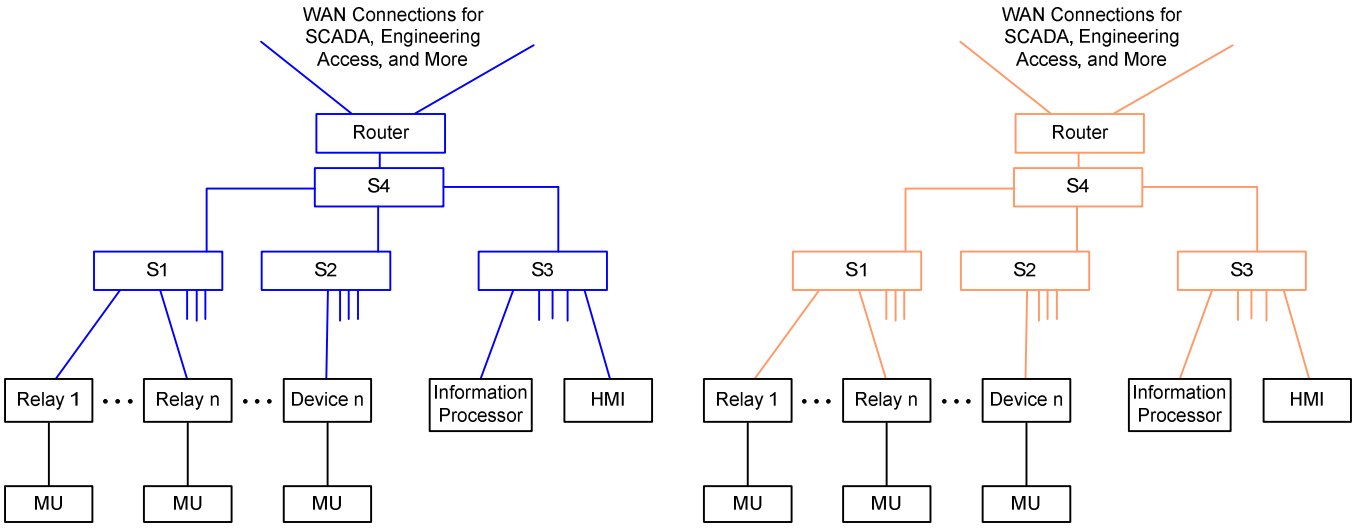

Fig. 8. Fully Independent Dual Networks With Redundant Devices and Point-to-Point Process Bus Links

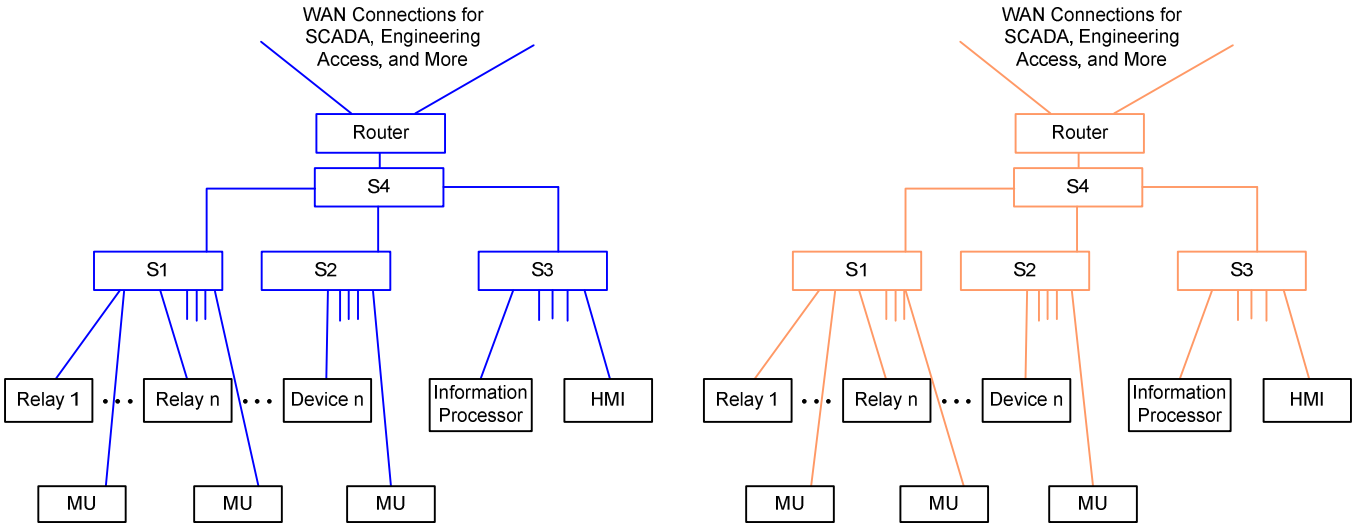

Fig. 9. Fully Independent Dual Networks With Redundant Devices and Network-Based Process Bus

V. Performance of Failover Methods

By comparing the application recovery times shown in Table I with typical network recovery times provided by the standard reconfiguration methods given in Section II, Subsection B, it is easy to see that the traditional Spanning Tree Protocol restoration time (30 to 50 seconds) is inadequate for power system applications.

The newest version of RSTP (RSTP-2004) works much better (30 to 60 milliseconds) and can easily satisfy engineering access, SCADA, time synchronization, and GOOSE-based automation applications. Fig. 10 shows the test configuration we used for recovery time measurements.

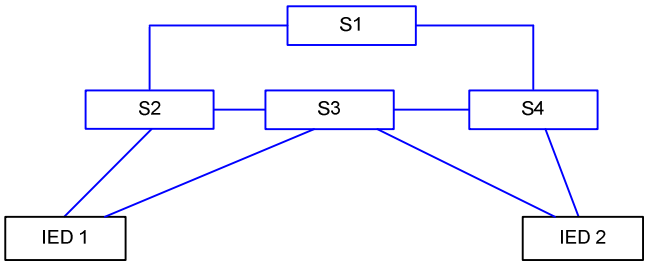

Fig. 10. Network Recovery Time Test Setup

Test results are consistent with literature, although some papers imply faster recovery (down to 2 milliseconds per switch).

The test results in Table II show that GOOSE message-based tripping, protection, and SV-based process bus applications need faster recovery, which cannot be met by RSTP. These applications are similar to industrial control systems and could potentially be addressed by borrowing some of the technologies developed for this field. As illustrated by the most recent industrial network standard [10], vendor competition unfortunately resulted in the development of six incompatible solutions that are being offered as a common standard.

Table II
GOOSE Service Restoration Time Test Results

Failure	GOOSE Service Restoration Time
Inactive Link	No loss of traffic
Active Switch Link	52 ms typical
Active IED Link	250 ms typical

The power system community, represented by IEC TC57 Working Group 10, is working to remedy this situation by developing a new proposal for seamless network recovery with no loss of data during network topology changes. This would be achieved by duplicating each outgoing message and sending it to its destination using two independent physical paths. Successful completion of this work should enable device interoperability, while ensuring seamless traffic delivery.

In addition to substation LANs, it is interesting to look at WANs linking multiple substations [11]. Such networks are typically implemented by sending Ethernet traffic through synchronous optical network (SONET) multiplexers with counter-rotating rings and protection-path switching. SONET ring recovery time is normally below 50 milliseconds and can be as low as 3 milliseconds with the equipment optimized for power system applications. The faster of the two provides adequate performance for most stringent line current differential protection applications.

VI. Reliability of Network Topologies

The most reliable configuration is a primary network for the primary devices and a fully independent backup network connected to a full set of backup devices [1], as described in Section IV, Subsection C and shown in Fig. 4. Virtually all EHV and only some HV transmission substations have fully redundant backup protection and monitoring devices. For other stations, cost tradeoff considerations lead to the evaluation of networks without redundant monitoring and protection devices.

To calculate the availability for each topology, we used the mean time between failures (MTBF) and calculated availability shown in Table III, from data in [12]. To analyze systems with specific components, use the MTBF from the component manufacturer and the methods described in [1] and [12].

Table III
Component Reliability Data

Component	MTBF	Unavailability (Parts Per Million [ppm])	Availability
Monitored Ethernet Cable	5000 years	1.1	99.9999%
Relay Ethernet Port	2500 years	2.2	99.9998%
Relay or Merging Unit	200 years	27	99.9973%
Ethernet Switch or Router	60 years	96	99.99040%

The comparison calculations are based on 22 local station relays. Table IV summarizes the unavailability of the Ethernet network for each of the topologies described in Section IV. The unavailability numbers are normalized as numbers multiplied by 10^{-6}. In other words, unavailability is shown in units of ppm of time. To aid in visualization, an unavailability of 561 ppm is 295 minutes in a year. This is, however, the statistical average. In reality, we would expect that one of ten systems in a year would experience one two-day outage. This is the equivalent of a network MTBF of 9.8 years, where failure is defined as the inability of the network to perform the required tasks with a mean time to repair (MTTR) of 2 days.

TABLE IV
SYSTEM RELIABILITY COMPARISONS

Topology	Unavailability ppm	
	Network Only	Network, Relays, and Merging Units
Single Network	561	1164
Single Network With Redundant Paths	265	868
Dual Networks With Failover	0.3	603
Dual Redundant-Path Networks With Failover	0.1	603
Independent Dual Networks With Redundant Devices	0.3	1.4
Dual Redundant-Path Networks With Point-to-Point Process Bus	0.1	1206
Independent Dual Networks With Redundant Devices and Point-to-Point Process Bus	0.5	1.6
Independent Dual Networks With Redundant Devices and Process Bus Network	0.8	2.3

VII. SUMMARY

In this paper, we identified the weaknesses in redundant failover schemes that are not addressed by the existing IEC 61850 standard and noted that IEC TC57 Working Group 10 is investigating new solutions. Until those solutions are standardized and embodied in off-the-shelf products, engineers must apply existing technologies and equipment to implement Ethernet networks.

We contrasted several topologies using available equipment and provided the tools to weigh the tradeoffs for specific alternatives and applications. Existing equipment can be successfully deployed in networks using switching failover methods for SCADA and other relatively low-speed applications. However, for real-time breaker control or high-speed, wide-area control systems, the recovery times are too slow. If we use Ethernet networking for these high-speed applications, only fully redundant systems that do not employ failover provide both the required performance and reliability.

VIII. ACKNOWLEDGMENT

The authors gratefully acknowledge the contributions of Stephanie Leggett for her network testing work.

IX. REFERENCES

[1] G. Scheer and D. Dolezilek, "Comparing the Reliability of Ethernet Network Topologies in Substation Control and Monitoring Networks," proceedings of the 2nd Annual Western Power Delivery Automation Conference, Spokane, WA, April 2000.

[2] M. Galea and M. Pozzuoli, "Redundancy in Substation LANs With the Rapid Spanning Tree Protocol (IEEE 802.1w)." Available: http://www.ruggedcom.com/pdfs/white_%20papers/rapid_spanning_tree_in_the_substation.pdf.

[3] *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges*, IEEE Standard 802.1D-2004, June 2004.

[4] *IEEE Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power System Substations*, IEEE 1613-2003, July 2003.

[5] *Communication Networks and Systems in Substations – Part 5: Communication Requirements for Functions and Device Models*, IEC 61850-5 2003, July 2003.

[6] V. Skendzic and A. Guzmán, "Enhancing Power System Automation Through the Use of Real-Time Ethernet," proceedings of the 15th Annual DistribuTECH Conference, San Diego, CA, January 2005.

[7] V. Skendzic, I. Ender, and G. Zweigle, "IEC 61850-9-2 Process Bus and Its Impact on Power System Protection and Control Reliability," proceedings of the 9th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2007.

[8] *High-Voltage Switchgear and Controlgear – Part 3: Digital Interfaces Based on IEC 61850*, IEC Standard 62271-3, June 2006.

[9] L. Andersson, K. Brand, and C. Brunner, "Reliability Investigations for SA Communication Architectures Based on IEC 61850," proceedings of the 2005 IEEE PowerTech Conference, St. Petersburg, Russia, June 2005.

[10] *High Availability Automation Networks*, IEC Standard 62439, May 2008.

[11] R. Moore and V. Skendzic, "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 Automation Conference, Spokane, WA, April 2006.

[12] G. Scheer and R. Moxley, "Digital Communications Improve Contact I/O Reliability," proceedings of the 7th Annual Western Power Delivery Automation Conference, Spokane, WA, May 2005.

X. BIOGRAPHIES

Veselin Skendzic is a principal research engineer at Schweitzer Engineering Laboratories, Inc. Mr. Skendzic earned his B.S. in Electrical Engineering from FESB, University of Split, Croatia; his M.Sc. from ETF, Zagreb, Croatia; and his Ph.D. from Texas A&M University, College Station, Texas. He has over 25 years of experience in electronic circuit design, has lectured at FESB, and spent over 20 years working on power system protection related problems. Veselin is a senior member of IEEE, has authored multiple technical papers and patents, and is contributing to IEEE standards. He is an active member of the IEEE Power System Relaying Committee (PSRC) and chairman of the PSRC Relay Communications Subcommittee.

Gary W. Scheer received his B.S. in Electrical Engineering from Montana State University in 1977. He worked for the Montana Power Company (MPC) and the MPC subsidiary, The Tetragenics Company, before joining Schweitzer Engineering Laboratories, Inc. (SEL) 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 division 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 and the ISA.