Modern Ethernet Failure Recovery Methods for Teleprotection and High-Speed Automation

D. Dolezilek, C. Gordon, D. Anderson, and T. Tibbals
Schweitzer Engineering Laboratories, Inc.

Presented at the
5th International Scientific and Technical Conference
Actual Trends in Development of Power System Relay Protection and Automation
Sochi, Russia
June 1–5, 2015

Actual Trends in Development of Power System Relay Protection and Automation
1–5 June 2015, Sochi (Russia)

Modern Ethernet Failure Recovery Methods for Teleprotection and High-Speed Automation

D. DOLEZILEK, C. GORDON, D. ANDERSON, and T. TIBBALS
Schweitzer Engineering Laboratories, Inc.
USA
dave_dolezilek@selinc.com

KEYWORDS

High-Availability Seamless Redundancy (HSR), Parallel Redundancy Protocol (PRP), Rapid Spanning Tree protocol (RSTP), virtual local-area network (VLAN), software-defined networking (SDN), OpenFlow™, redundancy, reliability, PRP Redundancy Box (RedBox).

1 INTRODUCTION

This paper compares the mechanisms for quickly reconfiguring Ethernet networks to satisfy mission-critical performance metrics while providing simultaneous duplicate or redundant signal exchange. This paper also compares the attributes and complexities of duplication methods and redundancy methods that are available in software-defined networking (SDN) to create lossless signal delivery with the use of Ethernet packets and address issues of teleprotection, interlocking, and automation applications based on IEC 61850 Generic Object-Oriented Substation Event (GOOSE) messaging.

Mission-critical protection signaling applications based on the IEC 61850 communications standard exchange signal statuses, alarms, and measurements as information within GOOSE messages. Redundancy to improve the availability of mission-critical applications is defined as the inclusion of extra components and capabilities—which are not strictly necessary for the application—to provide functionality in the event of failure within the primary system. Immediately after an intelligent electronic device (IED) senses a signal change of state, it publishes that change of signal information in a GOOSE message. In order to increase the dependability of teleprotection, interlocking, and automation, IEC 61850 describes a process by which IEDs make the new signal information redundant by publishing several redundant GOOSE messages consecutively in a burst after the initial change-of-state message, which is published immediately after a triggering event. These extra messages provide redundant signaling. Even if a network component fails immediately before the initial change-of-state GOOSE message is published, lossless signal transfer is attained with fast and efficient processing of the spanning tree algorithm (STA) and well-engineered Ethernet network topologies [1]. Using the ladder topology and fast STAs, network failures are detected and corrected quickly enough that one or more of the redundant GOOSE messages reaches each subscriber. Figure 1a illustrates a signal exchange where the first physical device (PD1) senses a change via a contact input and communicates the signal status change with a message published in an Ethernet packet. The Ethernet packet is sent through the network to the second physical device (PD2), which trips an output contact. Figure 1b illustrates the misconception that a second Ethernet cable connected to an IED provides a redundant connection. In order to avoid data flow loops, IEEE 802.1 Ethernet

mechanisms disable any second connection to an IED and force the connection into failover or hot-standby mode. This is a duplicate connection, not a redundant connection, because it is not active simultaneously with the primary link. The failover link only becomes active to publish GOOSE messages or any other Ethernet packets, and only after the primary connection has failed.

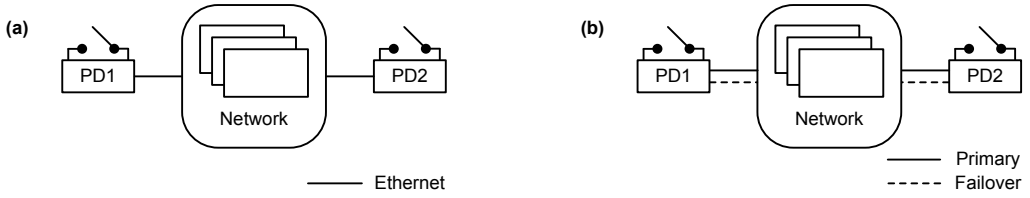

Figure 1: System Exchanging Protection Signals in Ethernet Packets Through a Network (a) and Duplicate Ethernet Cable Serving as Hot Standby (b)

Link failure detection and reconfiguration is traditionally performed by an STA based on information received within Rapid Spanning Tree protocol (RSTP) messages published by network devices on the shared Ethernet network. When the STA reconfigures the Ethernet network failure in less than 15 milliseconds, all or most of the redundant GOOSE packets are delivered and satisfy protection signal applications. Network devices between IEDs—referred to as middleboxes—with slower STAs cannot be relied on for mission-critical signaling. Some middlebox manufacturers offer proprietary solutions, but the solutions are not useful in systems including devices from multiple manufacturers because they are not standardized or interoperable. As a result, when middleboxes rely on slowly resolved STAs, manufacturers recommend purchasing and building two duplicate RSTP Ethernet networks in the hopes that while one network fails to deliver packets, the duplicate network will not fail simultaneously. Although simultaneous failure is not statistically likely, it is still possible, so it is important to use topologies that are more resilient than a simple ring [1].

2 COMMUNICATIONS-ASSISTED APPLICATIONS VIA DIGITAL MESSAGES

2.1 Signaling Requirements for Teleprotection, Interlocking, and Automation Applications

The hard-wired exchange of protection information uses an analog value at the receiver to indicate the logical status of the signal from the sender. Typically, an analog value of zero indicates a status value of zero and the maximum analog value represents a status value of one. This method creates a constant signal value at the receiver. However, if the signal wire is cut or disconnected, the receiving device cannot distinguish between this failure or a legitimate zero analog value. With digital messages, the signal exchange is not constant. Each time a digital message is received, the signal status is confirmed or a change of status is recognized. The receiver assumes that the signal status remains unchanged during the time between messages. However, the digital message exchange can be supervised, and the receiver detects when the communications link is lost. MIRRORED BITS® communications publish digital messages every 2 milliseconds over dedicated links, so the signal confirmation or a change of state is detected within 2 milliseconds at the receiver. Non-change-of-state GOOSE messages are typically set to occur once per second to act as an application heartbeat, and the time between signal confirmations at the receiver grows to once per second. A signal status change of state typically triggers an immediate GOOSE publication so, as with MIRRORED BITS, the change of state is detected within 2 milliseconds at the receiver when the network performs correctly and delivers one of the messages within the burst. In order to provide lossless signal transfer in the event of a network failure, IEC 61850 describes a method for the IED to send several redundant change-of-state indications in a burst of redundant messages after the change of state occurs. If the failure is corrected before the burst is complete, lossless signal delivery is achieved.

GOOSE heartbeat messages are not published more rapidly than the typical once per second to reduce the traffic on the shared-bandwidth Ethernet network. The consequence is that the time between confirmations is much longer, and the time it takes to detect failed communications is much longer than other digital messaging methods. Alternatively, a direct Ethernet connection between relays avoids the challenges of the shared purpose and bandwidth of the Ethernet network and performs more reliably. On a direct Ethernet link, GOOSE packets can be configured to be published

every few milliseconds rather than once per second, thus improving both application reliability and failure detection.

The IEC 61850 standard refers to the use of unique identifiers or virtual local-area networks (VLANs) based on IEEE 802.1Q, referred to as QVLANs, to be configured within GOOSE and Sampled Value messages. These message QVLANs, illustrated as tags in Figure 2a, are reviewed by the middlebox port connected to the GOOSE publisher to determine if the packet should be allowed to ingress the network. IP messages have no value in the message tag field and are referred to as untagged. When untagged messages ingress a middlebox, they inherit the port-based VLANs (PVLANs) configured on the middlebox port, as shown in Figure 2b. Both the PVLAN tag and the QVLAN tag identifiers are used by the middlebox to determine which port the packet is allowed to egress.

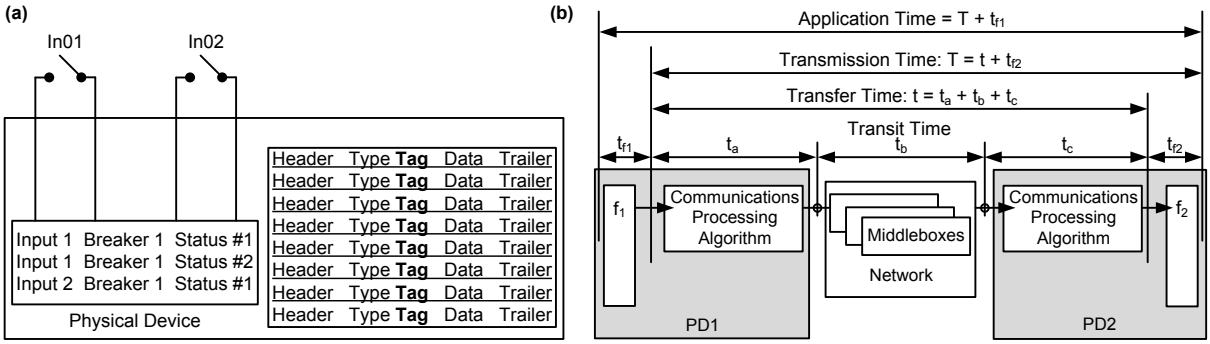

Figure 2: IED Contact Input Information Mapped as Payload Data in GOOSE Messages (a) and Application, Transmission, Transfer, and Transit Time Based on IEC 61850-5 (b)

The IEC 61850 standard also refers to the use of Type 1A Performance Class P2/P3 messages with a transfer time requirement of less than 3 milliseconds for digital signals as part of the communications-assisted protection scheme illustrated in Figure 2b. IEC 60834-1 requirements for security, reliability, and dependability are met if the system meets the 3-millisecond transfer time 99.9999 percent of the time and has a delay no longer than 18 milliseconds for the remainder [1]. The IEC/TR 61850-90-4 network engineering guidelines [2] for IEC 61850 Ethernet traffic suggest that GOOSE messages used for protection should be designed to have the highest priority and the shortest maximum delay. Control blocking schemes, via GOOSE messaging or any other method, require a 99.99 percent success rate, and direct control schemes require a 99.9999 percent success rate of the receipt of digital messages (reliability). Direct tripping through delivery and processing of a GOOSE or other message is typically expected to occur within a transmission time of 20 milliseconds [1]. Failure is defined by the absence of the message at the receiving end or, for direct control, a delay in delivery greater than 18 milliseconds. Therefore, the use of Class P2/P3 messages requires that the system be designed to meet the 3-millisecond transfer time. This requires high device reliability to keep the path failures to a minimum. System availability analysis based on IEC 61850-5 measures of reliability is used to predict the ability of each system to meet IEC 60834-1 dependability and security requirements [1]. For example, a GOOSE application configured to publish confirmation messages every second publishes 86,400 messages every 24 hours. Applying the IEC 60834-1 standard to a GOOSE signal exchange for direct tripping with a 1-second heartbeat requires that the network deliver every single GOOSE message packet (dependability) and deliver fewer than nine unwanted GOOSE message packets (security) during every 24-hour period [3].

2.2 Redundant Information, Messages, Packets, and Applications

The redundancy method with the highest availability as a percentage of expected run time is to create two complete and separate systems, isolated from one another, acting as dual primary redundant applications, as shown in Figure 3a. This provides complete application redundancy as well as redundant information, messages, and packets. In the event that completely redundant systems are not possible, adding a dual primary trip device (DPTD) makes the mitigation application redundant via the redundant trip function, as shown in Figure 3b. The information can be singular, or it can be redundant with a second contact input, as shown in Figure 2a. The message can be singular, or it can be

redundant if a second message is configured into the source device. According to IEEE 802.1, the packets are duplicated and rebroadcast within a middlebox when the same message is published to both PD2A and the DPTD. Therefore, additional redundancy is provided when two GOOSE messages are configured, one for PD2A and a redundant one for the DPTD.

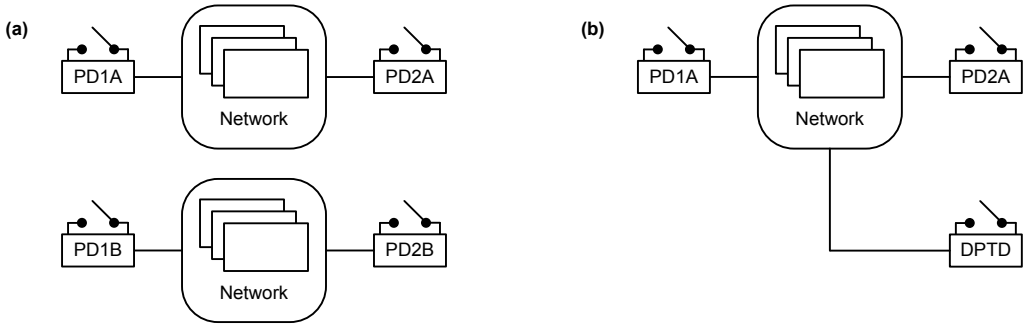

Figure 3: Complete Dual Primary Signaling Systems (a) and Application of DPTD (b)

2.3 Redundancy Protocols and Duplication Methods

Rather than improve the STA and network topology, many IED manufacturers have chosen to promote a variety of message duplication schemes in an attempt to provide lossless signal exchange during failure and recovery of links and Ethernet middlebox hardware [3]. In addition to the process of redundant GOOSE publications after a change of state, three methods are currently available to quickly overcome failures or create duplicate or redundant messages: STAs, IEEE 802.1Q message redundancy, and message duplication protocols. An emerging method, SDN, will soon be available for use in power systems and will dramatically improve digital messaging.

2.3.1 Fast STAs

Traditionally, STAs in each middlebox share data through the use of RSTP (particularly IEEE 802.1D-2004), which publishes Bridge Protocol Data Unit packets that communicate middlebox statuses to overcome failures. Using information from other middleboxes, each STA identifies and deactivates duplicate paths to a network address. Duplicate paths are forced into hot-standby mode and may be reactivated to reconfigure the network after a failure. The speed with which typical middleboxes resolve STAs is inadequate for protection and high-speed automation. Testing of a four-node ring of often-used middleboxes reveals transit latencies that grow from hundreds of milliseconds to tens of seconds. Without testing, most end users are unaware that their ring networks perform this poorly. Specific research and development have led to the use of the ladder topology, as shown in Figure 4a, and modern, faster, but still interoperable execution of the STA to ensure fast reconfiguration times [3]. During reconfiguration after a failed middlebox or link, the ladder topology with an interoperable and fast STA recovers every non-root bridge and many root bridge failure scenarios in less than 15 milliseconds. The remaining root bridge failures take a slightly longer time. However, any ring topology larger than three middleboxes with traditional STAs will not reconfigure in less than 15 milliseconds. The ladder topology with a fast STA is less expensive, simpler, and easily understood; and it provides much more resiliency than other methods. For example, the devices attached to middlebox switches B3 and B5 in the ladder network in Figure 4a are proven to have lossless signal exchange even if the network experiences up to five middlebox switches and ten link failures [1].

2.3.2 IEEE 802.1Q VLAN Methods

Using ingress filtering based on QVLANs for redundancy, it is possible to send GOOSE messages into two different networks connected to two different ports on the same device, as shown in Figure 4b. Both IED ports are active and connected to a different network, and data flow loops are prevented by IEEE 802.1Q filtering. The primary network is configured to allow all untagged IP traffic and GOOSE message packets tagged with QVLAN identifiers allocated to the primary LAN. This creates a fully functional primary network with GOOSE message burst redundancy. The second IED Ethernet port is connected to a redundant protection LAN that is configured to allow only tagged traffic with QVLAN identifiers designated for use on the protection LAN, as shown in Figure 4b.

These QVLAN tag identifiers must each be unique from tags allocated to the primary LAN, and the middlebox ports are also configured to deny Network A IP traffic. This redundant protection network is much simpler than the primary network because it only connects to the second Ethernet port of IEDs sharing signals. The information can be singular, or it can be redundant with a second contact input. The messages and packets are redundant. The QVLAN method is the simplest, least expensive, and most effective way to produce redundancy. Virtually all modern STA-based Ethernet middlebox hardware supports the well-established IEEE 802.1Q VLAN segregation method.

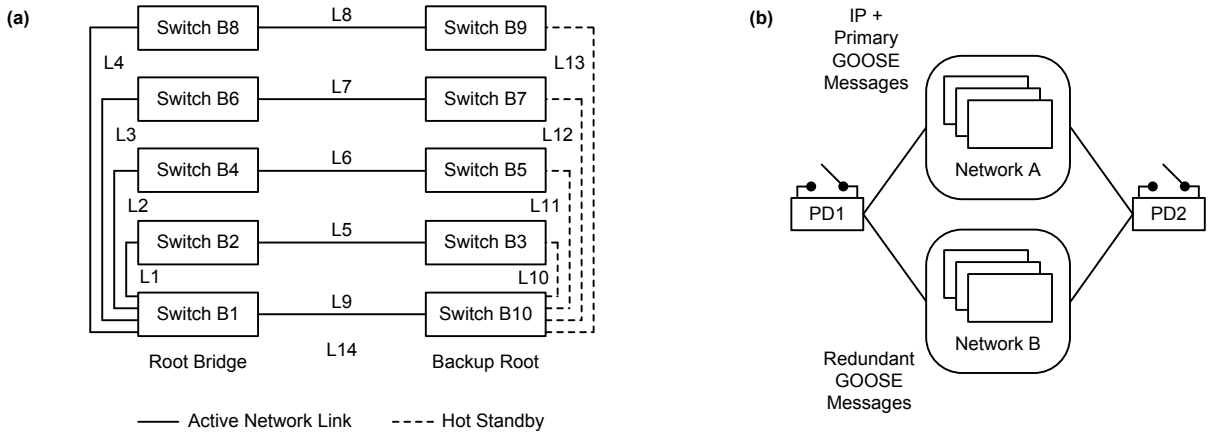

Figure 4: Dual Primary Signaling Via Two Systems Segregated by Way of QVLANS (a) and Resilient Single Primary Ladder Network Topology (b)

Single or redundant networks are enhanced to provide additional redundancy by way of dual primary contact inputs and DPTDs, as illustrated in Figure 5a and Figure 5b, respectively, which can be isolated via QVLANs.

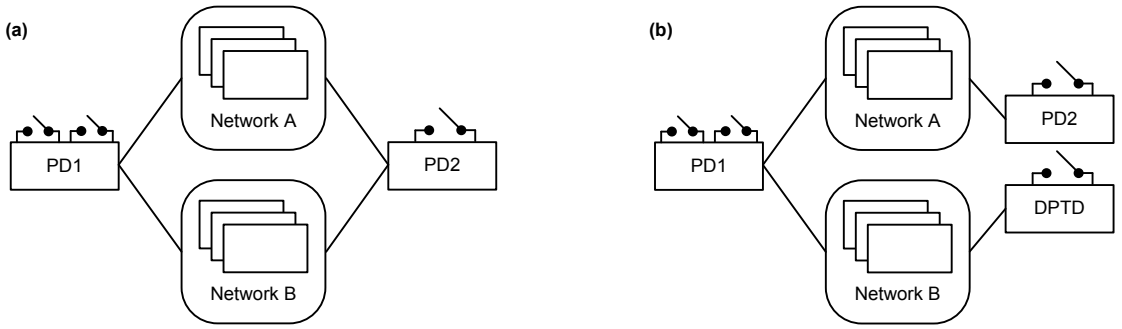

Figure 5: Redundant Information Via Dual Primary Contact Input (a) and Redundant Application Via DPTD (b)

2.3.3 Duplicate Ethernet Packets Via Parallel Redundancy Protocol (PRP)

Per Clause 4 of IEC 62439-3, PRP is an industrial Ethernet duplication method that is referenced by IEC 61850 [4]. This method does create redundant Ethernet packets but does not provide redundant applications, information, or messages. This method delivers duplicate messages through two separate networks, as shown in Figure 5a, which in this case are isolated via PRP. PRP enables source devices to create duplicate packets and publish them out two different Ethernet ports. PRP uses a redundancy control trailer (RCT) tag added to the end of an Ethernet frame payload to identify outgoing packets and keep track of incoming packets. The RCT identifies the sequential order of the message via the sequence counter, and it determines whether the message is destined for Network A or Network B via the line identifier.

The receiver uses the PRP RCT tag to identify the packet as belonging to Network A or Network B. Devices process one of the duplicate messages they receive—usually the first one—and discard the other. This creates additional publication and subscription processing and the need for a second duplicate Ethernet network. A PRP Redundancy Box (RedBox) receives the packets from

non-PRP devices, tags them, and publishes them into Networks A and B. It also receives the duplicate messages, strips the PRP tags, and forwards the messages to the non-PRP devices.

PRP methods deliver a single duplicate packet in the event of any failure within either Network A or B, but not both. PRP includes no recovery mechanisms, so packet redundancy is disabled while a failure exists. If both Networks A and B are affected by the same failure, such as damage to a cable tray or conduit, signaling is disabled altogether and no recovery occurs.

Again, PRP does not provide redundant applications, information, or messages. It only provides duplicate messages and redundant Ethernet packet delivery until the first network failure and, therefore, is often combined with STA recovery methods.

2.3.4 Duplicate Ethernet Packets Via High-Availability Seamless Redundancy (HSR)

Per Clause 5 of IEC 62439-3, HSR is an industrial Ethernet duplication method created for use with IEC 61784 protocols and adapted by some for IEC 61850 [4]. Like PRP, the HSR method creates redundant Ethernet packets and does not provide redundant applications, information, or messages. This method duplicates and delivers each IED message in two directions around a single ring network, as shown in Figure 6a. By duplicating every message, HSR reduces the effective network bandwidth and available device processing by 50 percent.

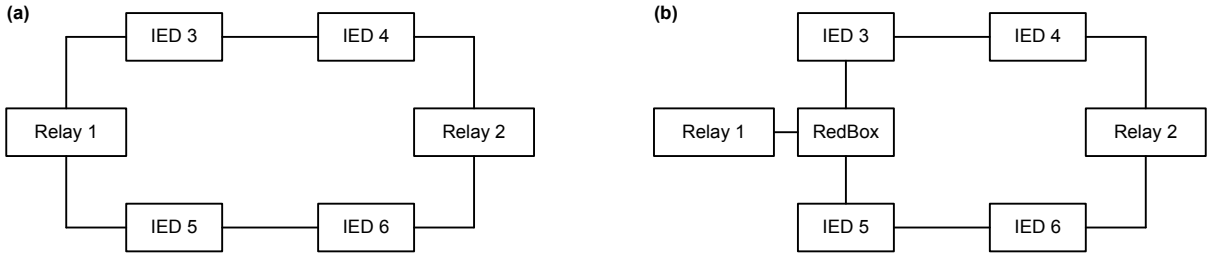

Figure 6: Redundant Packets Within Single HSR Network Ring (a) and Non-HSR-Enabled Relay Connected Via RedBox (b)

HSR-enabled source devices create duplicate packets and publish them out two different Ethernet ports. However, because HSR uses a tag added to the beginning of the message, it is no longer an Ethernet message and cannot travel through Ethernet switches. The HSR tag is used to identify outgoing packets and to keep track of incoming packets, and each device processes one of the duplicate messages it receives—usually the first one—and discards the other. This creates additional publication and subscription processing in each IED, which may slow the application and the delivery because each packet must pass through each IED. This method delivers a single duplicate packet in the event of any single failure within the ring. However, in the event of a second network failure, redundant messages and all communications will fail to reach the isolated segment.

The forwarding delay of every device in a HSR ring adds to the total network latency, so special hardware is often required to reduce the per-hop latency to a reasonable value. These device requirements make HSR very specialized, expensive, and potentially cause additional packet latency. Also, only half of the network bandwidth is available to applications because all frames are sent twice over the same network, even when there is no failure. Similar to PRP, non-HSR devices can be added through connections to a RedBox, which converts non-HSR packets into HSR and vice versa, as illustrated in Figure 6b.

HSR jeopardizes signal exchange because each device in the ring adds signal delivery latency, and every device must process and pass on each message in the network. The most difficult challenge is that, because there is no recovery method when a fault occurs on the ring, the network link remains broken until someone performs repair.

Both HSR and PRP can be connected together using RedBox interconnections. However, no combination will provide redundant applications, information, or messages.

2.3.5 SDN and OpenFlow™

SDN is a new architecture in networking that simplifies network management by abstracting the control plane from the data plane. Figure 7 illustrates the building blocks of SDN, which provide logical separation of creating and executing the data flow rules [5]. The SDN controller understands

the entire network and sends rules to the SDN middleboxes, which are programmed simply to execute the flow rules as directed by the controller. With SDN, the middleboxes no longer need to send RSTP messages or run STAs and can make much faster and deterministic decisions on where to send packets based on logical paths computed by the controller. Also, without STAs, the network is capable of managing more than one active connection to each end device. When two cables are connected to an IED, they are both allowed to function simultaneously and pass different or redundant messages on each link.

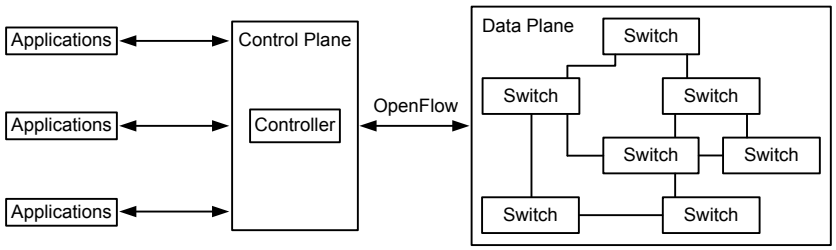

Figure 7: SDN Architecture Overview

SDN controls an entire network as a single operating environment and allows administrators to implement and operate the network in a way that is targeted directly at the end-needs of each application. SDN gives operators high-level control over individual message types by separating the brain that decides traffic flow from the hardware that pushes packets. OpenFlow is an increasingly popular protocol that acts as the interface between the SDN brain (the control plane) and the packet-pushing hardware (the data plane).

When using STA, each Ethernet middlebox is responsible for its own data flow decisions. This leads to a great deal of complication during dynamic conditions due to all the independent decision-making at one time. SDN (when implemented with OpenFlow) solves this problem because all states in the system—including those with host, link, and middlebox failures—may be precomputed by the SDN controller and implemented in OpenFlow-enabled middleboxes, eliminating the need for packet-pushing hardware to discover the state of the system from neighboring middleboxes.

OpenFlow provides three functions that help the controller make decisions on packets that ingress an Ethernet middlebox: matches, actions, and counters (or statistics). Combinations of matches and actions make up flow tables, while counters (collected by the controller via a poll) detail information such as byte counts, flow table matches, and more.

- OpenFlow matches: When an Ethernet frame first ingresses the middlebox hardware, the OpenFlow-enabled middlebox examines the packet in search of match fields. Match fields can be physical, such as physical ingress ports and packet headers found in OSI layers 2-4.
- OpenFlow actions: When a match is found for a particular flow table, actions can be performed. Actions may include traditional packet-handling methods, such as forwarding or dropping. OpenFlow also allows copying of frames to multiple end ports, the application of metering- or rate-limiting functions, and direct manipulation of packet headers.
- OpenFlow counters: OpenFlow-enabled middleboxes keep counters for every port, flow, flow table, and other logical and physical ports and actions performed. Examples of counter data can be the number of dropped frames, total byte count for a flow table, and so on.

OpenFlow has the ability to define the logical or physical data path for an Ethernet frame based on any matched packet field. OpenFlow can detect teleprotection messages by their Ethertype and treat them as critical traffic with unique data paths. For example, OpenFlow middleboxes may be programmed to send packets back out the port where the packet was received, which STA will not allow, in order to find a suitable egress port. OpenFlow can also copy ingressing critical frames and forward out multiple ports, or it can dedicate physical links for specific flows to minimize possible queueing or latency. Because OpenFlow can operate on either a blacklisting or whitelisting premise, it can also effectively firewall all communications. Furthermore, OpenFlow does not consume additional bandwidth or disable backup links because only specific traffic flows need to be made redundant, and all links may be used by OpenFlow hardware.

OpenFlow rules can be initiated on a schedule in order to enable maintenance modes where OpenFlow flow tables redirect all traffic around affected portions of the network without loss of data.

3 CONCLUSION

In order to provide lossless signal transfer in the event of a network failure, IEC 61850 describes a method for the IED to send several redundant change-of-state indications in a burst via republications after the change of state occurs. If the failure is corrected before the burst is complete, lossless signal delivery is achieved. Also, protection application operations are made redundant through DPTDs in the same network consuming the GOOSE message or another based on unique contact input information.

The most reliable application redundancy method is to provide two complete and separate systems, physically isolated from one another and acting as dual primary redundant applications. The second most reliable method is the use of redundant dual primary networks isolated by way of QVLANs. PRP provides duplicate information and GOOSE messages delivered by way of redundant Ethernet packets in duplicate networks. HSR provides no redundancy of application or information, but it does provide duplicate messages and redundant packets in a single-ring network. HSR and PRP can be combined in various topologies and connect traditional devices by way of RedBoxes. While PRP, HSR, and any combination of the two can provide redundant packets, they cannot provide redundant applications, information, or messages. Actual times of message transit during normal and failed network situations require specific staging and testing. Table 1 in the appendix compares the different methods based on capability and complexity.

Due to its flexibility, OpenFlow is the future “best in class” choice for teleprotection systems because OpenFlow switches make efficient use of existing links and simultaneously provide extremely granular control over passing Ethernet traffic.

4 REFERENCES

[1] S. Chelluri, D. Dolezilek, J. Dearien, and A. Kalra, “Understanding and Validating Ethernet Networks for Mission-Critical Protection, Automation, and Control Applications,” March 2014. Available: https://www.selinc.com.

[2] IEC/TR 61850-90-4, Communication Networks and Systems for Power Utility Automation – Part 90-4: Network Engineering Guidelines.

[3] D. Bekker, T. Tibbals, and D. Dolezilek, “Defining and Designing Communication Determinism for Substation Applications,” proceedings of the 40th Annual Western Protective Relay Conference, Spokane, WA, October 2013.

[4] IEC 62439-3, Industrial Communication Networks – High-Availability Automation Networks – Part 3: Parallel Redundancy Protocol (PRP) and High-Availability Seamless Redundancy (HSR).

[5] R. Bobba, D. R. Borries, R. Hilburn, J. Sanders, M. Hadley, and R. Smith, “Software-Defined Networking Addresses Control System Requirements,” April 2014. Available: https://www.selinc.com.

5 APPENDIX

Duplication and Redundancy Methods	Lossless Signal Delivery	Redundancy					Coexist Standard Ethernet	Require Custom Device Software	Require Custom Device Hardware	Increase Message Delivery Latency	Increase Failure Recovery Latency	Network Bandwidth Available	Added Network Cost
		Message Burst	Application	Signal Data	GOOSE Message	Ethernet Packet							
Single application and ladder network, fast STA (Fig. 1a, Fig. 1b)	Y	Y	N	N	N	N	Y	N	N	N	N	All	None
Single application, single ladder network, fast STA, dual input contacts	Y	Y	N	Y	N	N	Y	N	N	N	N	All	None
Dual application, single ladder network, fast STA, DPTD (Fig. 3b)	Y	Y	Partial	N	Y	Y	Y	N	N	N	N	All	None
Dual application, single ladder network, fast STA, dual input contacts, DPTD	Y	Y	Partial	Y	Y	Y	Y	N	N	N	N	All	None
Dual primary applications, physically separate networks (Fig. 3a)	Y	Y	Total	Y	Y	Y	Y	N	N	N	N	All	Double
Single application, duplicate GOOSE, dual primary networks isolated via QVLANs (Fig. 4b)	Y	Y	N	N	N	Y	Y	N	N	N	N	All	Double
Single application, dual inputs, redundant GOOSE, dual primary networks isolated via QVLANs (Fig. 5a)	Y	Y	N	Y	Y	Y	Y	N	N	N	N	All	Double
Dual application, dual contact inputs, redundant GOOSE, dual networks isolated via QVLANS (Fig. 5b)	Y	Y	Partial	Y	Y	Y	Y	N	N	N	N	All	Double
Single application, duplicate messages, fast STA ladder networks isolated via PRP (Fig. 5a)	Y	Y	N	N	N	Y	Y	Y	N	N	N	All	Double
Single application, duplicate messages, single ring network via HSR (Fig. 6a)	Y	Y	N	N	N	Y	N	Y	Y	Y	Y	One-half	> Double
Single application, duplicate GOOSE, dual primary paths within single SDN network	Y	Y	N	N	Y	Y	N	N	N	N	N	All	None
Single application, dual contact inputs, redundant GOOSE, dual primary paths within single SDN network	Y	Y	N	Y	Y	Y	N	N	N	N	N	All	None

Table 1: Summary of Metrics for Duplication and Redundancy Methods