Using Software-Defined Networking to Build Modern, Secure IEC 61850-Based Substation Automation Systems

Amandeep Kalra, David Dolezilek, Jerin Monzi Mathew, Rajkumar Raju, and Robert Meine
Schweitzer Engineering Laboratories, Inc.

Dinesh Pawar
Bharat Heavy Electricals Limited

Presented at the
15th International Conference on Developments in Power System Protection
Liverpool, United Kingdom
March 9–12, 2020

USING SOFTWARE-DEFINED NETWORKING TO BUILD MODERN, SECURE IEC 61850-BASED SUBSTATION AUTOMATION SYSTEMS

Amandeep Kalra[1], David Dolezilek[1], Jerin Monzi Mathew[1], Rajkumar Raju[1], Robert Meine[1], Dinesh Pawar[2]*

[1]Schweitzer Engineering Laboratories, Inc., Pullman, Washington, USA
[2]Bharat Heavy Electricals Limited, Bhopal, India
**dave_dolezilek@selinc.com*

Keywords: SOFTWARE-DEFINED NETWORKING, SUBSTATION AUTOMATION SYSTEM, IEC 61850, ETHERNET NETWORKS, CYBERSECURITY.

Abstract

Substation automation systems (SASs) are an essential part of smart grid systems. They consist of intelligent electronic devices (IEDs) communicating using digital communications protocols over a secure local-area network. Today, SASs can support multiple protection, monitoring, and control applications over the same network, allowing real-time decision making by various devices and fast reactions to ever-changing power system states, within a few milliseconds. Additionally, large amounts of data exchanged by devices in an SAS enable smart decision making by stakeholders and improve overall system performance and efficiency.

To ensure reliable operation of SASs, a highly secure and resilient communications network backbone is a must. Traditional Ethernet technology was not designed to meet the performance and reliability requirements that are essential for SASs. Moreover, an electric power system is an attractive target for cyber attacks, so modern operational technology (OT) Ethernet networks must be designed with security in mind to protect against cyber threats. In this paper, we discuss an application of software-defined networking (SDN) to meet stringent network performance and cybersecurity requirements. We compare this application to traditional spanning-tree-based networks to show SDN's ability to meet and exceed those requirements.

1 Introduction

A large power generation utility in Gujarat, a state in western India, contracted Bharat Heavy Electricals Limited (BHEL) to design a modern IEC 61850-based substation automation system (SAS) solution for their new 800 MW coal-based thermal power station. The utility had strict performance requirements for an Ethernet network to support various power system applications. Moreover, the utility wanted to adopt an innovative approach to secure the Ethernet network from the ever-increasing threat of a cyber attack.

Considering the performance, security posture, and features of operational technology (OT) software-defined networking (SDN), BHEL proposed an SDN solution as part of the SAS. In this paper, we discuss the process of engineering a modern IEC 61850-based 400 kV SAS using SDN to fulfill the utility's requirement of building a secure, reliable, resilient, and scalable Ethernet network.

We begin by discussing the performance requirements of this application. We then compare the traditional Ethernet network approach of using Rapid Spanning-Tree Protocol (RSTP) to SDN—based on the criteria of security, reliability, network visibility, scalability, and changeability—to explain why SDN was the best solution. Then, we discuss the engineering design process and decisions, as well as the implementation of an OT SDN network that meets and exceeds the requirements and also achieves redundancy and resiliency for simultaneous network faults without IEC 62439-3 Parallel Redundancy Protocol (PRP). Finally, we discuss potential future enhancements to add more cyber intelligence to the IEC 61850-based SAS by using intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) in coordination with SDN to detect, deter, and mitigate cyber threats.

2 Network Specifications and Performance Requirements

The SAS design for the utility's thermal power station, simplified as Fig. 1, required interconnecting control and protection systems at a 400 kV air-insulated substation extension bay; a 400 kV gas-insulated substation (GIS); and an 800 MW generator, with a generator transformer, a unit transformer, and station transformer protection panels in the central control room. All 58 IEC 61850-compliant intelligent electronic devices (IEDs) in the network had to communicate with the two supervisory control and data acquisition (SCADA) servers in the GIS control room. These servers provided the data for visualization and control to human-machine interfaces (HMIs) located in all three control rooms.

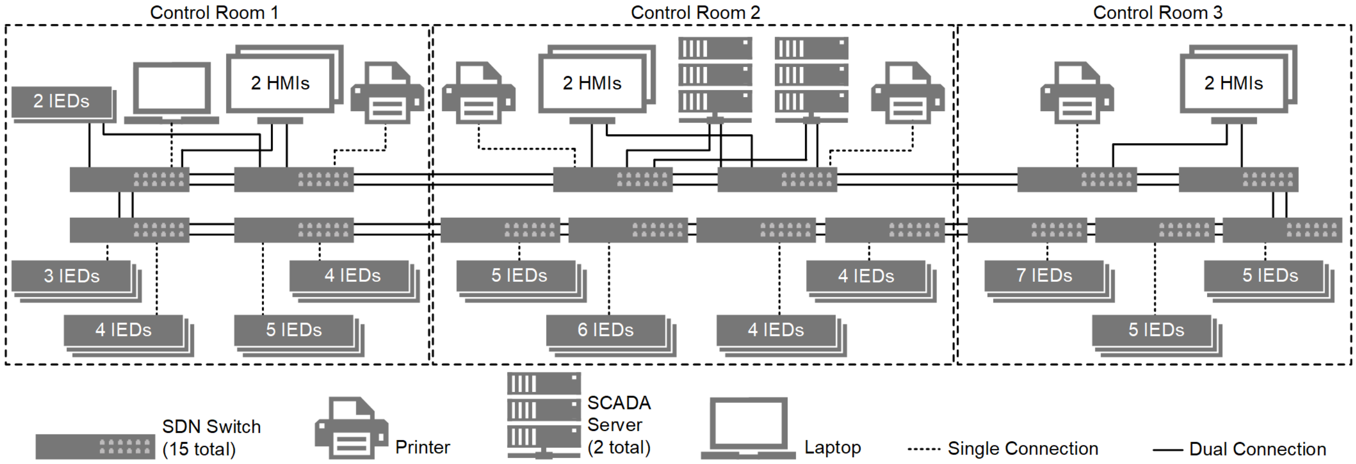


Fig. 1. Simplified network topology of SAS.

Critical system data were sent via the SCADA servers to the thermal power plant distributed control system and the state load dispatch center, using IEC 60870-103 and IEC 60870-101 or IEC 60870-5-104 protocols. Also, the IEDs in the network needed to exchange IEC 61850 Generic Object-Oriented Substation Event (GOOSE) messages to provide control interlock and protection functions.

A communications network of this scale must provide the required performance and detailed monitoring through the SAS network to validate the performance. It needed to provide traffic isolation, prioritization, and cybersecurity to ensure smooth operation and monitoring of the entire SAS. Monitoring the communications network was also necessary to provide accurate information about communication link health and to generate alarms in the event of a link failure.

Per IEC/TR 61850-90-4 network engineering guidelines and IEC 61850-5 communications requirements, trips and blockings must be transferred within three milliseconds and releases and status changes transferred within ten milliseconds for optimum performance, as Table 1 shows [1] [2]. Thus, during a failure of any link in the dual-ring topology, the network must fail over to an alternate path quickly, without degrading the performance of other applications running on the network.

Table 1 IEC/TR 61850-90-4 network engineering guidelines: performance and test

Transfer Time Class	Transfer Time (ms)	Application Example
TT0	Less than 1,000	Files, events, and log contents
TT1	1,000	Events and alarms
TT2	500	Operator commands
TT3	100	Slow automatic interactions
TT4	20	Fast automatic interactions
TT5	10	Releases and status changes
TT6	3	Trips and blockings

3 Brief Introduction to SDN Technology

SDN is an architectural networking concept that abstracts the control plane (responsible for deciding how to forward Ethernet frames) out of the data plane (the SDN switches that forward the Ethernet frames) and centralizes it in software, as shown in Fig. 2 [3]. This central software is called an SDN controller and manages the fleet of SDN switches in its domain.

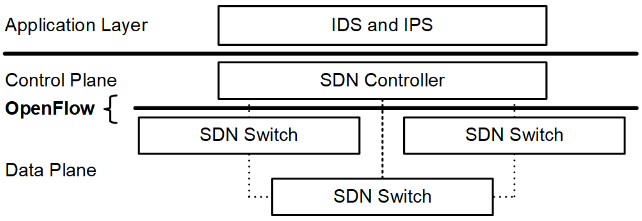


Fig. 2. SDN architecture.

OT SDN differs from information technology (IT) SDN by its use of proactively engineered flow entries for both the primary and failover paths. OpenFlow is a protocol the SDN controller uses to configure the OpenFlow-based SDN switches, which operate on a match-action scheme, to control how SDN switches forward Ethernet frames. As frames enter the switch, they are matched against a set of rules (i.e., matches) predefined by the end user. The matches can be anywhere from Layer 1 to Layer 4 of the Open System Interconnection (OSI) model, as shown in Fig. 3. Depending on which rule matches the Ethernet frame, it is either dropped or egressed from the switch (i.e., actions). A match-action pair is called a flow entry [3] [4]. If an Ethernet frame does not match any flow entry, the packet is discarded, making it a deny-by-default filter.

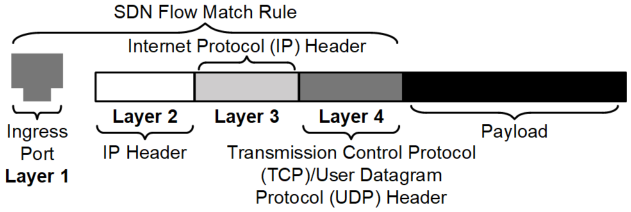
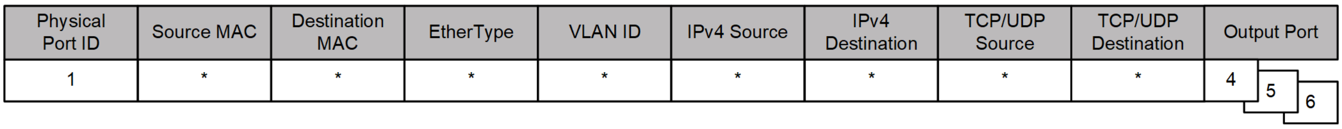
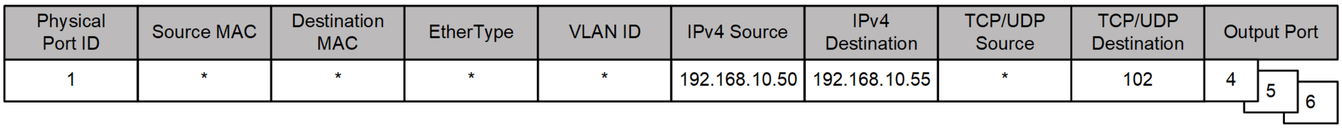

SDN Flow Match Rule
Internet Protocol (IP) Header
Ingress Port
Layer 1
Layer 2
IP Header
Layer 3
Layer 4
Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) Header
Payload

Fig. 3. Layer 1 to Layer 4 of the OSI model.



Physical Port ID	Source MAC	Destination MAC	EtherType	VLAN ID	IPv4 Source	IPv4 Destination	TCP/UDP Source	TCP/UDP Destination	Output Port
1	*	*	*	*	*	*	*	*	4 5 6

Fig. 4. Layer 1 Ethernet frame filtering.



Physical Port ID	Source MAC	Destination MAC	EtherType	VLAN ID	IPv4 Source	IPv4 Destination	TCP/UDP Source	TCP/UDP Destination	Output Port
1	*	*	*	*	192.168.10.50	192.168.10.55	*	102	4 5 6

Fig. 5. Multilayer Ethernet frame filtering.

In the example shown in Fig. 4, a flow entry is programmed to match all traffic entering Port 1, regardless of any other matches (marked with an *) that may differ. The associated action assigned is to egress the traffic out Port 4 as the primary path, out Port 5 if Port 4 is down, or out Port 6 if both Ports 4 and 5 are unavailable.

Fig. 5 shows an example of a multilayer match. This match designates that all the IEC 61850 Manufacturing Message Specification (MMS) Ethernet frames incoming on Port 1 have IPv4 source address 192.168.10.50, IPv4 destination address 192.168.10.55, and TCP/UDP Port 102. The associated action is to egress this traffic from the designated output, Port 4, with backup paths on Ports 5 and 6 available, as in Fig. 4. Additional flow entries could be present to match other Ethernet frames, providing application-focused, multilayer frame inspection at every hop for strong network access control.

Users manage the network configuration through the SDN controller to provide single-asset management of the network. The SDN controller then manages the configuration of the switches. The switches will operate without communication with the SDN controller because they retain their configuration in persistent flow tables. These flow tables contain both the primary and failover paths, so the switch can immediately react to a network disturbance without needing to communicate with the control plane. Because of this, network healing time during any link or switch failure may be less than 100 microseconds [5].

By managing flow entries, the network prevents unauthorized applications from running, thus improving system cybersecurity. This also helps prevent broadcast storms in the network, saving bandwidth for critical applications.

4 Comparison of Traditional and SDN OT Networks

OT networks in substations and industrial control systems are responsible for supporting critical processes and high-speed decision making. To support this, machine-to-machine (M2M) communication in a substation, such as IEC 61850 GOOSE messages, requires a reliable communications network.

Traditional Ethernet switches have both a control plane and a data plane. Each switch learns the media access control (MAC) addresses and locations of its neighboring devices by examining entering Ethernet frames. The traditional switch then dynamically maintains that information in MAC tables and uses it to forward Ethernet frames to learned destinations. This provides plug-and-play capabilities to end device traffic but can also lead to bandwidth consumption when flooding multicast and broadcast traffic.

Traditional networks use RSTP for loop mitigation in ring network topologies. The loop mitigation built into RSTP technology enables redundancy, but it also logically disables ports to avoid loops, as shown in Fig. 6, reducing the efficiency of the switch and increasing the total cost of ownership.

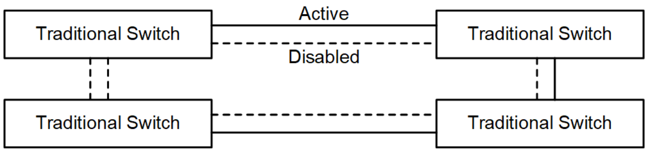


Fig. 6. Dual-ring topology with RSTP loop mitigation.

The deny-by-default Ethernet frame-forwarding mechanism of SDN, in comparison to flood-by-default in traditional networking, helps to avoid loops in the network, without the need for RSTP. This is because the failover path is precalculated and operates immediately after the network disturbance without the need for control plane convergence. Without RSTP, no ports are logically blocked to prevent loops. This allows users to utilize the total bandwidth provided by the ring or dual-ring network. For example, in a dual-ring network, users can configure flow entries to allow only GOOSE messages in one ring and SCADA traffic in the second ring when both rings are healthy, as shown in Fig. 7.

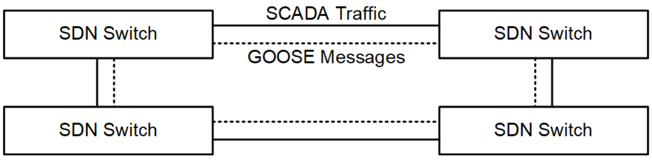


Fig. 7. Dual-ring topology with SDN.

In a critical communications network carrying M2M messages, it is best practice to reduce the number of hops between devices and to have multiple paths to reach the destination. Mesh topology, shown in Fig. 8, is ideal for such situations.

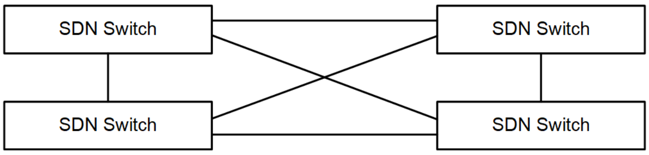


Fig. 8. Mesh topology with SDN.

In traditional Ethernet networks, mesh topology is not recommended because it creates multiple loops, further complicating the RSTP convergence process, and it increases network healing time. In contrast, SDN switches can utilize any enabled port in a mesh network to provide fast failover, which results in a high network resilience. The fast failover and advanced traffic management features of SDN enable a network engineer to uniquely design the physical topology to optimize the application needs. Network reconfiguration activates the redundant path not only when any ring port or traditional switch in the network experiences a failure but also when an Ethernet cable is removed to add a new switch or IED.

Healing time in an RSTP-based network depends on the network topology, RSTP configuration, and the number of traditional switches in the network, but it is typically between 5 and 100 milliseconds. In most cases, the healing time of any link failure is between 10 and 30 milliseconds [3] [4]. During the network healing period, existing application communications may be disrupted. This does not provide the resilience required for critical protection applications.

RSTP networks overcome the unacceptable healing time by duplicating the network, as mentioned in [6], and by sending duplicated Ethernet frames through the separated networks to the end destination. During a failure in one network, Ethernet frames from the other network will reach the destination without any network healing time delays. The scope of the PRP standard is limited to single network failure, unless a compensating failover mechanism such as RSTP is used to address multiple simultaneous failures.

Because the healing time of an OT SDN network is well below the time requirements for TT5- and TT6-class traffic (see Table 1), an OT SDN network may not require PRP to provide the required performance, thus reducing the cost of ownership. However, if both operate together, SDN improves the capabilities of a PRP network. As Fig. 9 shows, two devices in PRP mode are communicating over LAN A and LAN B using the same physical Ethernet switch but different logical paths, designated by differently patterned lines. The failover paths for LAN A and LAN B are shown as solid lines. SDN can interconnect independent paths through LAN A and LAN B without mixing duplicated Ethernet frames, thus providing higher reliability in case of multiple failures in the network. It can also accommodate multiple converging or independent failover paths for both LANs.

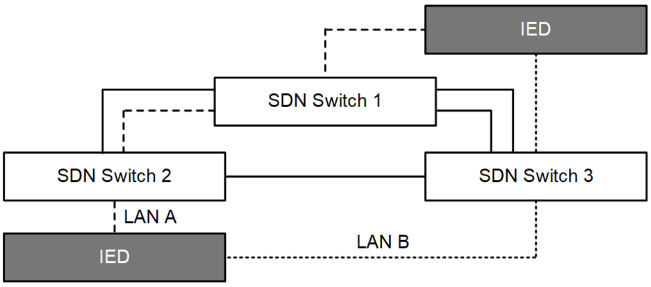


Fig. 9. Enhancing PRP network with SDN.

Cyber risks to OT networks are real and have catastrophic consequences, as seen during the 2015 attack on the Ukrainian grid [7]. These risks are often intensified if the control system networks are unmanned and exist in geographically remote places. Having deny-by-default Ethernet frame filtering using SDN enables engineers to approve which services are running on a network, reducing network exposure and, thus, risk. Any new communications flow added to the network, such as a new protocol or device must be approved by a network engineer before it can communicate with other devices [3]. Since SDN switches use persistent flow tables instead of dynamic MAC tables, they are safeguarded against various cyber attacks, as mentioned in [8].

Refer to Table 2 for a brief summary of the features of traditional and SDN networks discussed in this section.

Table 2 Comparison of traditional and SDN network

Comparison	Traditional RSTP	OT SDN
Failover time	Depends on topology	Less than 100 microseconds
Ethernet frame filtering	Layer 2 switches are different from Layer 3	Layer 1 to Layer 4 Ethernet frame filtering
Ethernet frame forwarding	Based on MAC tables	Match-action
Cybersecurity	Allowed by default	Deny by default
Failover behavior	Reactive	Proactive

5 Designing and Deploying the Network

Before creating a network engineered for device applications, we first needed to identify the applications and protocols the utility uses, the devices using the applications, and the network topology. This is because, in a proactively designed network, OpenFlow entries are tailored to the needs of device applications, along with their associated network protocols, including SCADA interactions with the switches themselves.

We deployed the SDN installation at the utility with the following steps:

1. Design the network.
    a. Gather data regarding the devices, applications, and topology.
    b. Based on these data, create path plans and determine policy.
    c. Develop the OpenFlow programming that fits the policies and data.
2. Validate and test that configuration against the requirements.
3. Deploy the configuration to the network.

After we deployed the initial configuration using these three steps, we entered change requests to modify the documentation of the network configuration, which begins a new cycle. The overall process is shown in Fig. 10.

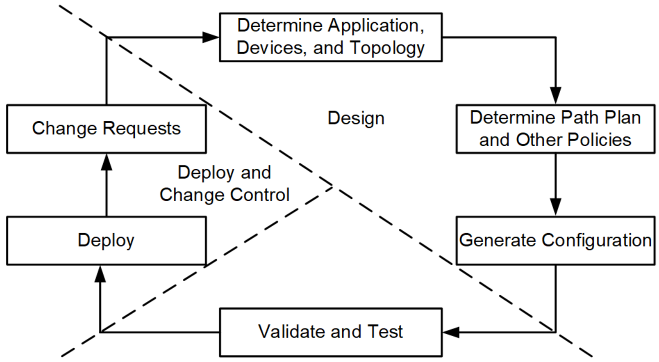

Determine Application, Devices, and Topology
Design
Change Requests
Determine Path Plan and Other Policies
Deploy and Change Control
Deploy
Generate Configuration
Validate and Test

Fig. 10. Network design and deployment process.

5.1 *Data Collection*

For this project, the commissioning and network engineers collected the data needed for the network engineering from the substation configuration description file and spreadsheets of device settings, which included device names and IP addresses.

5.2 *Path Planning and Other Policies*

After compiling the needed data, our next step was determining each path the Ethernet frames would take. Because it is a dual-ring topology, each hop left and right has two possible paths. Thus, frames egressing from a switch on the rings had four potential paths: two rings and two directions per ring. GOOSE traffic was assigned to one ring, and the remaining traffic—IPv4 and ARP—was assigned to the other ring to physically segregate the two types of traffic, shown in Fig. 11.

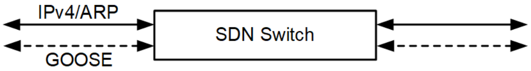


Fig. 11. Traffic allocation across two data paths.

Using this allocation, the latency of GOOSE through the network would be unaffected by the load of IPv4 traffic under normal operation. OT SDN provides the flexibility to operate on an even more precise level. Some of the IPv4 traffic allowed between two devices was only MMS if, due to security policies, MMS was the only communications type designed between the two devices. Based on the distribution of devices around the rings, we used the shortest path to determine which direction to forward Ethernet frames on the ring, as this provided an even distribution of traffic.

Another necessary path planning consideration is designing accommodations for network disturbances, such as a downed link or switch. In the instance of a downed link in the primary path, we designed the switch to temporarily forward the traffic from one ring onto the other ring for that hop. Priority is then managed not by physical segregation but by the priority queue, with GOOSE traffic assigned the higher priority. If instead, the next switch is down so that both forward paths are down, then the Ethernet frame is sent in the reverse direction. In this manner, a frame will reach its destination if at least one path is available. Fig. 12 shows an example of an IPv4 Ethernet frame path during a network disturbance.

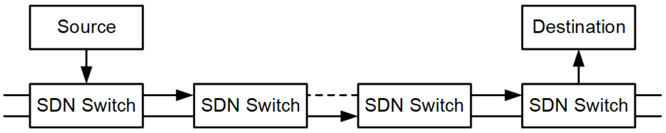


Fig. 12. IPv4 failover path plan.

5.3 *Validating and Testing the Network*

Before applying the engineered configuration to the physical switches, we first needed to validate that this configuration met the system requirements and test that the applications operated as specified. By validating and testing the configuration before applying it to the production network, any potential issues can be identified and addressed more quickly.

There are two parts to validating the network: validating that the traffic of all device applications reaches its assigned destination and ensuring that the network demands do not exceed the resources of the SDN switches.

Because SDN switches rely on persistent match and action schemes for forwarding decisions on the data plane, tools can simulate Ethernet frames to validate whether a frame entering the appropriate port will egress only from the designated port in a predictable manner.

Using a tool to simulate traffic, we validated each Ethernet frame's primary and failover paths by simulating link and switch failure. For security testing, we injected spoofed frames to confirm they did not reach any device. In this manner, we tested each path to confirm that the Ethernet frames only enter their expected destinations, even during network disruptions. Once the tool reported satisfactory results, we programmed the complete network in the lab according to specifications. This allowed us to both physically test the network behavior during a network event and test the network commissioning process.

5.4 *Deploying the Network*

After validating and testing the configuration, the network engineer passed the configuration to the commissioning engineer through a backup of the configuration. The commissioning engineer then commissioned each switch using the configuration and inserted the switch into the network. Once the network is fully deployed, the commissioning engineer can confirm that all communications are operational.

6 Maintenance and Change Control

Any system must support maintenance and change control requests after the network is deployed. Before or after the site is commissioned, the commissioning engineer may need to make changes to one or more parts of the network design.

To do so, the network engineer and commissioning engineer adhere to the following process:

1. Commissioning engineer updates the documentation.
2. Network engineer creates, validates, and tests the new configuration, as applicable, and sends the new configuration to the commissioning engineer.

3. The commissioning engineer imports the new configuration, synchronizes the switches, and checks communications.

The changes are applied as a differential so that the original configuration is modified as little as possible to minimize application disruption. If another switch is added to the network, the process remains the same: update the documentation, generate and validate settings, and then add the new switch and synchronize the rest.

If an engineer needs to replace a switch, the switch is removed from the network, its configuration is applied to the replacement switch, and then the new switch is inserted into the network. Because of the preconfigured entries in the remaining switches, traffic is not disturbed outside of the narrow range during which the switch was removed.

7 Future Enhancements

In addition to the SAS for the new 800 MW generation unit and associated substation, the power generation company has 1,470 MW of generation from seven existing 210 MW units and their associated 400 kV substation. In the future, the SDN network can easily expand to integrate the IEDs in the existing units and substation with the new SAS without disturbing the current network. Because SDN does not add any extra header or trailer to the Ethernet frames, it is easy to integrate legacy Ethernet-based devices with modern Ethernet-based devices in an SDN network. This is much more economical than in a PRP and High Seamless Redundancy (HSR) network configuration, which requires using external redundancy boxes, also called RedBoxes, to dually connect non-PRP/HSR devices to a PRP/HSR network [6].

Also, because SDN is managed through a centralized control plane, it is much more conducive to the application of an IDS and IPS, which would greatly improve network cybersecurity. With SDN, the network can push all or some Ethernet frames to the IDS without relying on a bump-in-the-wire system. IDS and IPS systems, alongside the honeypot over the control plane, are designed to effectively thwart cyber intrusions.

8 Conclusion

This paper describes how SDN is used to build secure, resilient, and high-performance Ethernet networks for IEC 61850-based SASs and other OT applications. The necessity to provide fast failover, data segregation, and cybersecurity, coupled with the geographic separation of the three control rooms in the project, prompted the utility in Gujarat to choose an SDN-based dual-ring topology to establish their SAS network. This network consisted of 80 devices—including 58 IEDs and 8 SCADA computers—singly and dually connected to 15 SDN switches. This paper also discusses our holistic process for configuring and testing this SDN network.

SDN technology is very simple to understand and use. It allows for the exact configuration of a network to be automated using various tools and configuration software. It creates networks that are future-proof in terms of expandability and provides real-time, centralized visibility into the network, including the number and type of devices connected, the communications protocols, and the number of Ethernet frames exchanged from every device for each type of protocol. In addition, the failover performance of SDN can reach times of less than 100 microseconds, regardless of the network topology and size, providing fast failover without additional protocols.

Based on these findings, the authors recommend the use of this technology in all Ethernet communications-based OT applications to build robust, secure, and resilient networks.

9 References

[1] IEC/TR 61850-90-4, Communication Networks and Systems for Power Utility Automation, Part 90-4: Network Engineering Guidelines, Technical Report, 2013.

[2] IEC 61850-5, Communication Networks and Systems for Power Utility Automation, Part 5: Communication Requirements for Functions and Device Models, 2013.

[3] Meine, R.: “A Practical Guide to Designing and Deploying OT SDN Networks,” proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2019.

[4] Bobba, R., Borries, D. R., Hilburn, R., et al.: “Software-Defined Networking Addresses Control System Requirements,” April 2014. Available: selinc.com.

[5] Chelluri, S., Dolezilek, D., Dearien, J., et al.: “Understanding and Validating Ethernet Networks for Mission-Critical Protection, Automation, and Control Applications,” March 2014. Available: selinc.com.

[6] IEC 62439-3, Industrial Communication Networks—High Availability Automation Networks, Part 3: Parallel Redundancy Protocol (PRP) and High-Availability Seamless Redundancy (HSR), 2016.

[7] Whitehead, D. E., Owens, K., Gammel, D., et al.: “Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies,” proceedings of the 70th Annual Conference for Protective Relay Engineers, College Station, TX, April 2017.

[8] Risley, A., Carson, K.: “Low- or No-Cost Cybersecurity Solutions for Defending the Electric Power System Against Electronic Intrusions,” April 2006. Available: selinc.com.

20191108 • TP6959