# Software-Defined Networking Reinforces Security and Performance in Operational Technology Communications Networks

Anwar Habeeb Moinudeen and Ammad Ali
*Schweitzer Engineering Laboratories, Inc.*

Presented at the
GCC Power 2019 Conference & Exhibition
Muscat, Oman
October 27–29, 2019

# SOFTWARE-DEFINED NETWORKING REINFORCES SECURITY AND PERFORMANCE IN OPERATIONAL TECHNOLOGY COMMUNICATIONS NETWORKS

Anwar Habeeb Moinudeen* and Ammad Ali
*Schweitzer Engineering Laboratories, Inc.*

USA

***Summary*—Utilities and industrial plants are concentrating on enhanced security and performance in communications network technologies, which has provided new opportunities for managing critical data.**

**This paper discusses the basics of control and data planes in a network system. It also compares software-defined networking (SDN) performance with that of traditional Ethernet switches and discusses how SDN optimizes the network in an automation system. This paper discusses OpenFlow, one of the most popular SDN southbound protocols. This paper also discusses how new SDN technology enhances operational technology (OT) communications network performance, security, configuration, and management. It shows how an SDN network protects using communications protocols such as IEC 61850 Manufacturing Message Specification (MMS), Generic Object-Oriented Substation Event (GOOSE) communications, IEC 61850-9-2 Sampled Values (SV), and Precision Time Protocol (PTP).**

***Keywords*—Software-defined networking (SDN).**

## I. Introduction

Modern communications networks have grown increasingly complex, making it challenging to meet today's strict requirements. Software-defined networking (SDN) is a new approach that addresses the weaknesses of the current paradigm [1]. Recently, the interest in SDN has extended into the operational technology (OT) networks responsible for critical infrastructure.

Since the first Ethernet switch was released in 1980, there have not been many enhancements to the IEEE 802.1 bridging standard [2] to strengthen security and flexibility. Ethernet technology is common in information technology (IT) networks and in OT networks, like substation automation systems that have IEC 61850 Manufacturing Message Specification (MMS) and Modbus Transmission Control Protocol/Internet Protocol (TCP/IP) technology in the end devices.

The introduction of SDN to OT networks provides many traffic engineering benefits, such as more security and flexibility, predetermined path selection, simplicity, ease of use, predetermined recovery, and a higher quality of service (QoS). TCP/IP-based systems are pivotal in supervisory control and data acquisition (SCADA) networks as power utilities migrate their traditional networks to centralized control centers, which require robust, reliable, and nearly deterministic operational behavior.

The key applications commonly used in substation networks include IEC 61850 MMS, Modbus TCP/IP, DNP3 over TCP, and File Transfer Protocol (FTP). Some of these applications, particularly IEC 61850-based substation automation systems, dictate strict requirements for network operation performance. It is difficult for traditional networks to meet the performance requirements of typical electrical power systems. Moreover, as utilities continue to upgrade their OT networks, traditional networking technology continues to face challenges, such as handling shared bandwidth with control systems.

Traditional networks participate in a distributed decision-making process to create and enforce a network hierarchy. In loop avoidance mechanisms, switches use Spanning Tree Algorithm (STA), which runs in the background of Rapid Spanning Tree

*Schweitzer Engineering Laboratories, Inc., 2350 NE Hopkins Court, Pullman, WA 99163 USA • papers@selinc.com

Protocol (RSTP) and Spanning Tree Protocol to determine the root bridge. The root bridge is a reference point for all switches in the spanning tree topology. The failover time depends on the number of nodes and the type of topology. These features make hardware more complex. Simplicity, ease of use, and automatic recovery were the goals of Ethernet technology, but according to [1], "as the scale and complexity of networks grew, the current model has become increasingly dysfunctional."

This paper examines how OT SDN can enhance security, flexibility, and traffic engineering. It focuses on building application-based, proactive deny-by-default networks. OT SDN does not change the basic architecture of SDN but is rather a way of applying SDN to solve challenges in OT networks composed of devices such as programmable logic controllers (PLCs) [3]. Such networks are often used for critical infrastructure, which focuses on reliability, security, and real-time performance.

This paper also discusses how OT SDN technology can be efficiently used to deploy IEC 61850-based systems on process-level protection-class Ethernet networks (PCENs). Fast message transfer, which is used to achieve protection over communications networks, is driven by standards like IEC 61850-5 and will be discussed further in this paper.

In addition, this paper describes the SDN fast failover function with IEC 61850-9-2 Sampled Values (SV) and Generic Object-Oriented Substation Event (GOOSE) communications and how the traffic can be easily monitored in the SDN network using an intrusion detection system (IDS). This paper provides an overview of OT SDN, compares OT SDN with IT SDN, and shows how OT SDN can meet OT network requirements.

## II. How SDN Works and the Difference Between OT SDN and IT SDN

SDN is a network architecture that separates the data plane from the control plane. The control plane is considered the brains of the network. It is responsible for managing the information in the forwarding table and for processing control plane protocols like Address Resolution Protocol (ARP) and RSTP and routing protocols like Open Shortest Path First (OSPF). The data plane is used for reception and for forwarding packets through a switch. The forwarding functionality—including the logic and tables for choosing how to manage incoming packets based on characteristics such as media access control (MAC) address, IP address, and virtual local-area network (VLAN) ID—resides in the data plane. Fig. 1 shows the roles of each plane [1].

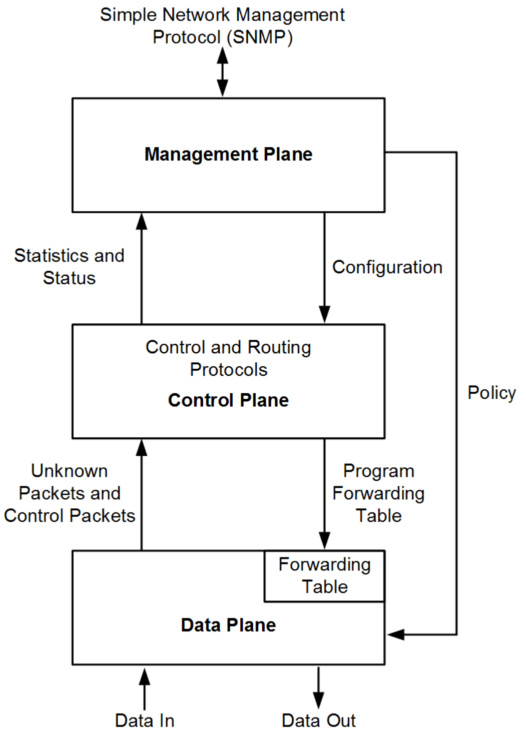


Fig. 1. Roles of control, data, and management planes.

In traditional Ethernet switches, control plane software in the switch determines the optimal path and responds to outages and new networking demands. The control plane runs the routing or switching protocols to synchronize the network. Placing more functionality in the hardware provides an all-in-one device but also makes that device more complicated because it simultaneously handles packets and decides their path [1].

In SDN, the control plane is not in the switch. Instead, it is placed in centralized software (referred to as the SDN controller or flow controller) that can see the entire network. This centralized system runs the management and control software instead of having complicated control plane software in each switch [1].

SDN networks are characterized by the following:

- Control and data plane separation
- Device simplification
- Centralized control
- Network automation
- Virtualization and openness

Fig. 2 shows the SDN architecture.

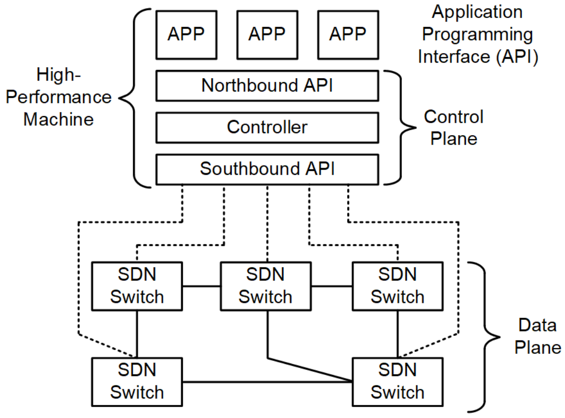


Fig. 2. SDN architecture.

The SDN controller communicates to the SDN switches through a southbound interface, and the controller communicates with operation, administration, and management applications through the northbound interface.

The origins of IT and OT SDN are the same, but they each apply SDN differently to address the challenges of critical infrastructure [1]. OT SDN networks are often used for industrial control systems, which focus on reliability, security, and real-time performance. Some applications cannot tolerate network failures greater than 20 milliseconds. The OT SDN deny-by-default feature makes the OT network more cybersecure, and fast healing provides real-time enhancements in the OT network.

Because OT networks are more persistent (i.e., changes occur very rarely and in a controlled manner), when the communications protocols between end devices are known, it is possible to whitelist the flows in the switches. In OT SDN networks, the ports the intelligent electronic devices (IEDs) are connected to are known in advance, as are the communications protocols to and from each device. Therefore, plug-and-play learning mechanisms like those use in IT networks are not necessary. To achieve reliability, multiple redundant network flows can be proactively engineered to achieve the predictable and deterministic behavior desired for such PCENs.

Table I shows the main differences between IT and OT SDN.

TABLE I
OT SDN VS. IT SDN

| Key Attribute | OT SDN | IT SDN |
|---|---|---|
| Network state | Persistent | Dynamic |
| Network control | Purpose-engineered | Traffic-reactive |
| Controller purpose | Monitor | Control |
| Security | Deny-by-default | Forward-by-default |
| Fault healing speed | Link detect | Flow setup time |
| Network management | Proactively planned | Fault-reactive |

## III. Packet Handling in OT SDN

In SDN, the control plane is extracted from the hardware and placed in centralized control plane software. Traditional switches integrate the control plane and data plane into the same device.

The following are advantages of centralizing the control plane [1]:

- Simplified traffic engineering and monitoring of network policies
- Reduced network appliance complexity
- Increased performance and determinism

The SDN controller programs the SDN switches with match (such as an ingress port, source and destination MAC addresses, a VLAN ID, or source and destination TCP or User Datagram Protocol [UDP] ports) and action (e.g., forward or drop) pairs to apply against incoming traffic.

The combination of match and action pairs is called a flow entry. Flow entries are the building blocks in SDN for traffic engineering the network. Traffic engineering involves proactively configuring all the packets that traverse the OT network under normal or failure conditions [1]. SDN switch traffic management depends on predefined flow entries. The match fields are either protocol- or layer-related, and they handle traffic based on the switch packet inspection up to Layer 4 and the user-defined criteria for those match fields.

As shown in Fig. 3, an SDN switch looks for a flow entry that matches an incoming packet [1]. If a match is found, the switch applies the associated action to the packet. If no match is found, it drops the packet by default or sends the packet to the controller, depending on the switch configuration. This makes the SDN technology suitable for OT PCEN applications where dynamic switch behavior is not required. SDN can match packets on network Layers 1 through 4, so each application up to and including the transport layer in the Open System Interconnection (OSI) model can be identified.

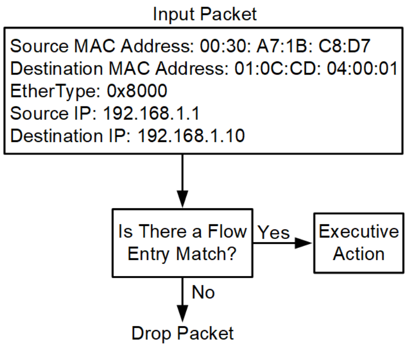

Input Packet
Source MAC Address: 00:30: A7:1B: C8:D7
Destination MAC Address: 01:0C:CD: 04:00:01
EtherType: 0x8000
Source IP: 192.168.1.1
Destination IP: 192.168.1.10
Is There a Flow Entry Match?
Yes
Executive Action
No
Drop Packet

Fig. 3. Basic packet-forwarding mechanism in SDN [1].

## IV. OpenFlow Overview

OpenFlow is an open standard protocol for programming the SDN switch data plane. OpenFlow was developed by the Open Networking Foundation (ONF). ONF was created to accelerate SDN switch delivery and commercialization. It manages OpenFlow specifications and releases. It originally was intended for the research community to serve as a platform for open network switching experimentation.

OpenFlow defines both the communications protocol between the SDN data plane and control plane and part of the data plane behavior, as shown in Fig. 4. The secure channel is the path used for communications between the OpenFlow controller and switch.

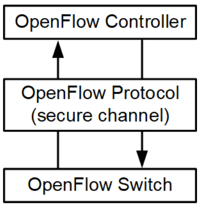


Fig. 4. Basic OpenFlow communications diagram.

## V. OT SDN Performance

### A. Healing and Reconvergence in Proactive and Reactive Networks

SDN uses multilayer packet matching and programmable instructions to forward packets and uses proactive engineering to avoid traffic loops rather than depending on STA.

STA performance in traditional networks depends on the number of devices in the network as well as the topology used. STA misconfigurations can affect the whole network. STA provides redundancy and recoverability at the time of a single point of failure, but this depends on how remaining network devices handle the healing situation. Networks can heal in milliseconds but may take seconds in the worst cases, such as when the root bridge fails in networks with many nodes. Root bridge failure induces large time delays and consumes useful network bandwidth to reconverge to a new root bridge. This can be harmful for time-critical PCEN networks because signals like Precision Time Protocol (PTP), GOOSE, and SV are present on the same path at a fixed rate with a constant heartbeat.

Traditional switches keep propagating the Bridge Protocol Data Unit (BPDU), which consumes a constant bandwidth in the network (unlike SDN, which does not require OpenFlow to transmit on a continuous heartbeat). Moreover, a traditional network provides less redundancy, which limits the resilience of the network and makes it difficult for the network to take an outage.

SDN healing time with fiber-optic links or 100 Mbps copper links is uniform across the network. The network topology does not impact the healing time in the SDN network. Because the SDN switches do not have a convergence time, no topology change mechanisms or root bridge elections need to be processed when a link or switch fails. In some situations, healing occurs in less than 100 microseconds [4]. This is a significant improvement in network healing time compared with traditional networks, which typically take more than 10 milliseconds. This high performance allows the OT owner to use even the most demanding applications, where signal loss can occur if network outages extend past half a millisecond, like with SV.

### B. Packet Integrity and Delivery

Packet integrity and delivery are measured by how accurately and fast the packets are delivered from the source to the destination. In an OT network, the time it takes for a packet to go from the source to the destination is as important as the integrity of the packet. Packet integrity means that there are no changes in the data in transit.

SDN does not have to look for the shortest path to the destination because the path for each destination and the *n* number of backup paths are predetermined and proactively engineered. Multilayer packet matching can identify each application until Layer 4 in the OSI model, making the network more secure. In OpenFlow, there is no MAC address table or routing table. Instead, as previously mentioned, the SDN switches look for flow entries that match incoming packets and apply the associated flow entry action to these packets.

In traditional network switches, the incoming packets are forwarded based on the destination MAC address. Whenever a new packet arrives, the source MAC address is stored in the MAC address table. If the destination address is not found in the MAC address table, the switch floods the traffic to get the reply from the destination address. There is also a limit to the number of MAC addresses that a single switch can learn. If that limit is exceeded, then the MAC address table overflows. Attackers can use these traditional switch limitations to gain access to a network.

Individual devices in the network have a maximum age time-out to flush out the MAC address table and to relearn the MAC addresses after a time. The device relearning process relies on an ARP broadcast packet. This can vary the time for packet delivery, which can be critical in OT networks. Also, this consumes useful bandwidth whenever any new device is connected in the traditional Ethernet network. This can lead the network to oversubscribe at the egress ports, which causes buffering in switches and can increase latency. If oversubscription persists for a long time, saturation can occur when internal buffers are exhausted, and packets are then discarded. However, in an OT SDN network, this behavior is controlled by pre-engineered flows. This helps mitigate broadcast storms and any related saturation. In SDN, the cast type for each packet does not affect how the packet is sent (i.e., unicast packets can be sent to multiple destinations, and multicast packets can be sent to a single destination).

With proactive engineering in the network, the switch knows how to correctly forward packets using the appropriate action, so there is no need to maintain a MAC address table or to flood a packet out every port. This removes the extra burden on the communications network. SDN switches do not need to figure out how to forward individual packets anymore because the system is predetermined by the centralized SDN controller. This improves network performance because different applications can use different paths to reach the same destination, and it removes the bottleneck issue that occurs in the traditional network switches.

### C. *Traditional Networks Limit the Number of Nodes*

Traditional networks limit the number of switches used in a ring topology that runs STA. STA based on IEEE 802.1 limits the switch placement to a maximum of 40 hops from the root bridge [4]. As discussed, the number of nodes increases the healing time. Also, with a larger, flat Layer 2 STA network, a broadcast storm adversely affects the performance of the entire communications system.

SDN does not limit the number of nodes in the communications network. No root election process occurs, and there is no issue of a newly added switch becoming a root. It is free from the complicated STA process. (SDN and STA can still coexist in a network with clear boundaries.) SDN switches do not require listening, learning, and forwarding stages. Once the link is up, SDN switches forward packets if they match any of the flow entries.

### D. *SDN and Parallel Redundancy Protocol (PRP)*

SDN can be used in systems where end devices use redundancy protocols like PRP. SDN is fully capable of handling packet flows as the user defines them. For example, in PRP networks, LAN A and LAN B can be defined logically in the OT SDN network by controlling the flow match rules, and they can have multiple or duplicated paths to the destination and vice versa. However, the SDN switch can still work as a transparent Ethernet packet transfer device to transport the PRP packets seamlessly, while ensuring fast failover, determinism, and resiliency.

## VI. Cybersecurity

The factors that can affect the network security and risk involved in OT networks are different from those in IT networks. The risk mitigation schemes depend on the variety of IEDs used in substation networks. Following networking best practices and threat modeling, OT systems can be managed to reduce the risk of cyber attacks. There are multiple standards and guidelines form organizations like ISO, IEC, NIST, NERC, and IEEE that dictate certain cybersecurity requirements in IT and OT networks. NERC CIP drives OT security to be deployed in power system Ethernet networks. NERC CIP requirements attempt to formalize best practices, threat assessments, and reaction planning.

Traditional networks often lack cybersecurity because they were developed for plug-and-play functionality. They were built to make the communications easy for network engineers, and they do not have much to do with traffic engineering. Most of the critical features are handled in the control plane with the help of different protocols. ARP is used to identify the link layer address. SNMP or a similar protocol is used for network management. These technologies have been used for a long time and have their own security limitations. Traditional network switches permit all traffic by default. These switches inspect packets once they arrive, and they continue to process the packets without confirming that the traffic is legitimate. A hacker can use these vulnerabilities to create disturbance in the network.

The cybersecurity performance of both Ethernet and SDN technologies can be evaluated by reviewing how they behave with known vulnerabilities and the security control in each technology.

Cybersecurity and risk management is a continuous process in any organization. It is driven by the constant introduction of new threats and advancement of technology. As the requirements of integrated solutions increase, cyber threats increase as well. In OT networks, the threats can be handled efficiently by using the right piece of equipment from the bay level of the OT architecture. The defense-in-depth concept is vital for OT security because it introduces multiple layers of security from an external network to the most critical infrastructure (e.g., station bus and process bus).

Cyber attackers are always looking to exploit vulnerabilities in traditional Ethernet networks. For example, attackers can use MAC table flooding to force a switch to refresh its MAC table [5]. Whenever an Ethernet switch receives a frame, it checks the MAC address table, records the source MAC address in the table, and checks if the destination MAC address is available in the table. If it is not, the switch forwards the frame out of all the ports in the switch except the one it received the frame from, like a hub. The vulnerability is that MAC address tables are limited in size. MAC flooding makes use of this limitation to send fake source MAC addresses to the switch until the switch MAC address table is fully loaded and cannot save any more MAC addresses. The switch then enters a fail-open mode, which means that it starts acting as an unmanaged switch. In this situation, the switch broadcasts all received packets to all the switch connections that are physically up. As a result, the intruder can see all the frames in the network. The only way to mitigate this is to enable the port security technology to bind the MAC address. The drawback to this is that a device with a unique MAC address in the network interface card for the device failover mechanism can cause an issue in the redundant Ethernet technology network. Replacing the device for maintenance to manage the MAC address binding adds extra cost and time.

### *A. Denial-of-Service (DoS) Attack Using TCP SYN Flood*

In a denial-of-service (DoS) attack, an attacker can overload system resources to significantly slow the system performance or to shut it down. The goal of a DoS attack is not to gain unauthorized access to a system or to corrupt data. Instead, it prevents a legitimate user from using the system. A SYN flood is a type of DoS attack where an attacker sends a large number of SYN requests to target a server with fake IP source addresses. The attacker creates incomplete TCP connections that consume network resources. In a normal TCP handshaking condition, the client sends a SYN packet to the end device to initiate the connection. The end device then responds to the SYN packet with a SYN/ACK packet. Finally, the client sends an ACK packet to acknowledge the receipt of the packet from the server (see Fig. 5) [6].

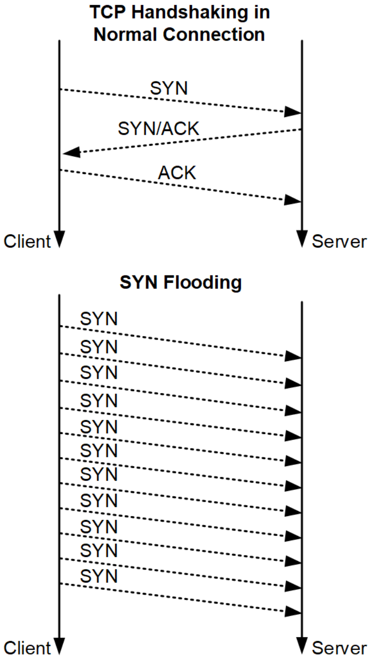


Fig. 5. TCP three-way handshaking and SYN flood process.

SYN flooding takes advantage of the vulnerabilities in TCP three-way handshake implementation. The attack occurs when the intruder continuously sends SYN requests to the server. The process of transmitting these packets is faster than the end device can handle. The server then responds to each of the connection requests and leaves an open port ready to receive the response. The server waits for the final ACK packet, which will never come [6]. In traditional networks, the packet keeps processing as it reaches the switch so the switch continues to receive the TCP SYN message and is sent to the server. DoS attacks may be targeted to prevent any or all use of a network.

In SDN, there are no similar control plane vulnerabilities because SDN switches are deny-by-default switches. MAC flooding and DoS attacks do not work in SDN because there is no MAC address table. TCP packets are not forwarded by default. They are instead forwarded based on flow entries, so any illegitimate packets are dropped by default. Vulnerabilities can be minimized in a persistent OT network with SDN.

SDN control planes are encrypted and authenticated. Communications in SDN are configured in the control plane, which is an authenticated and encrypted mechanism that reduces the attacking space and protects all legitimate management packets. In the OT SDN control plane, the controller is not required all the time in the network. Once proactive engineering is completed for the entire network, the control plane can be removed from the network and the data plane can manage the packets as programmed.

SDN can provide more cybersecurity than a traditional switch because it can filter up to Layer 4 in the OSI model. This means switches can match an incoming packet up to and including the transport layer. The more match fields added in the flow entries, the more secure and deterministic the traffic in the network will be. In an OT network, this helps limit the data flow in the network, and critical applications can be prioritized for higher availability.

### *B. IDS in an OT Network With SDN Technology*

The OT network security issue has increased drastically in recent years, and the number of cyber crimes in OT are increasing quickly. According to [7], "The increase attack in the [industrial control system] (ICS) environment shows it's a definite target for the hackers. How to protect the security of ICS is one of the most urgent Issue in the OT communication network." Different users make use of different technologies to bring security into their networks, such as implementing a firewall or Layer 3 devices (e.g., routers or Layer 3 switches) that segregate the network or implementing a different network monitoring tool like an IDS. According to [7], "IDS[s] are designed for the automatic detection of malicious attacks. They collect and analyze network traffic, security logs, audit data, and information from key points of a computer system, to check whether there exit security violations in the system. Intrusion detection is also one of the most important means of maintaining the security of ICS." An IDS can perform deep packet inspection up to the application layer.

As described previously, multilayer packet matching in SDN allows an optimized OT IDS to be deployed (see Fig. 6). Only illegitimate packets get inspected [5]. A rule can be created in the SDN controller to forward the packet to an IDS when there is no matching flow entry. This helps identify what is happening in the network. If the packets are legitimate but not allowed, then they can be easily identified and flow entries can be added to deliver the packets correctly. Also, the packet type can be used to identify DoS and other types of attacks. This adds another layer of security in the core network without adding dedicated, expensive devices (such as a stateful firewall) at a low level of the OT network infrastructure.

The simple QoS rate limiting meter feature in OpenFlow can be used in SDN switches. This can limit the number of packets sent to the IDS during a DoS attack rather than flooding the packets to the IDS or to the SDN controller. The meter (shown in Fig. 6) is defined on a per-flow basis.

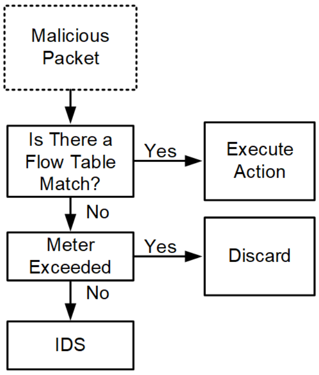


Fig. 6. IDS model in SDN.

Deploying an IDS in an SDN network is much easier than in a traditional network. An IDS is difficult to deploy in critical infrastructure that uses Ethernet technology because the IDS needs frequent signature updates and the Ethernet switch needs to span a port in the network to send all the packets to the IDS, which can increase the network overhead.

Multilayer packet matching permits the enforcement of OT protocol behavior to protect against mistakes and insider threats. If a packet is sent to the IDS, it must be identified because the purpose-engineered network was not engineered for that packet. There can only be two causes for this: either network engineers missed a legitimate packet and need to add flow entries for it, or there was an unauthorized packet on the network and its origin needs to be identified and isolated. It is very clear that SDN provides tremendous advantages in cybersecurity over traditional switches. The default purpose-engineered and predictable whitelisted technologies in the switch give a cybersecurity-embedded device category.

### C. *Maintenance, Testing, and Network Management Ease in SDN Technology*

Precommissioning testing in a traditional RSTP network is a cumbersome task that power utilities have to perform. The design and testing tools they use identify the worst-case scenarios in networks at live substations. Simultaneous substation events and network path failures can result in unique scenarios, which are challenging to test in factory-staged networks or to prevent in traditional OT networks. However, testing is more organized with SDN flow controller software, which reduces deployment times and eliminates human errors by programmatically testing the network implementation and validating the configurations before onsite deployment. This provides more flexibility and better visibility and is a more proactive approach to verifying critical networks.

The main challenges in the OT communications network are maintenance and network management. Engineers are forced to depend on third-party software to manage and maintain the OT network communications infrastructure. Replacing switches is time-consuming and expensive. With SDN technology, the SDN control plane is centrally located, which makes maintaining and managing the OT network much easier. When a switch needs replaced, it must be removed from the controller, and the new switch must adopt the previous switch configuration, which is already present in the controller. There is no need to back up the switch configuration individually. Normally, during a maintenance window, third-party manufacturers are given access to the OT network. This is a great problem in terms of cybersecurity. The application cannot be restricted for the third-party manufacturer in a traditional Ethernet network.

In SDN, only a specific protocol is allowed for the third-party manufacturer (e.g., Telnet). OpenFlow has a feature to automatically remove the flow entry for a particular match after a fixed time. This makes it easier to maintain and manage the OT communications network.

## VII. How SDN Technology Benefits IEC 61850-Based Substation Communications Networks

With the efforts to have intelligent protection and control IEDs integrated for coordinated electrical schemes spread over larger geographical areas, Ethernet emerged as a suitable message transport mechanism. Electrical communication over Ethernet enabled devices to share data and convert them into a useful database using data concentrators to visualize and operate the system on a larger scale from a centralized location. This integrated solution is a SCADA system, and it uses suites of protocols like IEC 61850 MMS, Modbus TCP/IP, DNP3 over TCP, FTP, Telnet, and others.

SCADA systems include protocols that are typically used to achieve time synchronization (e.g., Network Time Protocol [NTP]), digital and analog data retrieval and control (e.g., IEC 61850 MMS), and large file retrievals over networks (e.g., FTP). In most applications, SCADA systems do not require extremely high-speed networks, alarms, or 500 milliseconds for operator command execution, as explained in IEC 61850-90-4 guidelines.

However, this is not the case for integrated solutions, which contain peer-to-peer protection trips and blocking signals and use the same network as a SCADA system for high-speed control applications. Such networks need to be designed so that latency on a healthy network and failover on a faulty network do not exceed certain limits.

For control signals, according to [8], "IEC 61850-5 identifies Type 1A GOOSE Trip as most critical fast message in the substation that perform high-speed automation, protection and interlocking to meet or exceed a transmission of 3 milliseconds as Type 1A, Performance Class P2/P3." GOOSE is used for protection that has the highest priority and shortest maximum delay. Control blocking schemes via GOOSE or any other method require a 99.9999 percent success rate for receiving digital messages. 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, IEC 61850 Type 1A, Performance Class P2/P3 requires that the system meet the 3-millisecond transmission time 99.9999 percent of the time with no delay longer than 18 milliseconds during failover, which is one power cycle. The challenge is to create an Ethernet system that delivers packets quickly and reliably with minimal additional delay due to Ethernet interface, cable, or switch failure. This requires high device reliability to keep path failures to a minimum [9].

As shown in Fig. 7, GOOSE is designed to publish continuously in the network at a fixed heartbeat (T0). Once there is an event, which can be any protection trip or block, that has been assigned to GOOSE intertransmission between IEDs, GOOSE publication will be faster (i.e., at the rate of minimum time set T1, then double this time, and so on). This is to make sure that the receiving GOOSE IED has a greater chance of receiving the signal in case it misses a signal or two.

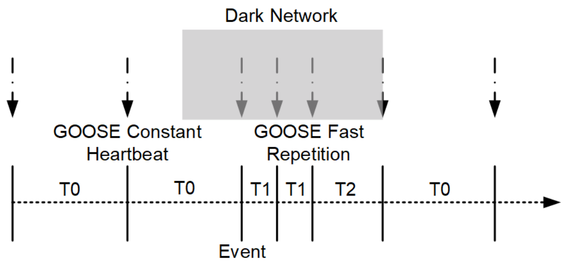


Fig. 7. GOOSE tolerance.

If the minimum time set is 4 milliseconds, then 4-, 4-, and 8-millisecond retransmission occurs initially. When there is network darkness during the event, the receiving IED may have a darkness period of greater than 16 milliseconds. This can be detrimental when the trip should occur within one power cycle (i.e., 20 milliseconds in a 50 Hz system). The period of darkness may be larger when Ethernet networks have many nodes or there are poor RSTP configurations. Moreover, after the broken link comes up or the network reestablishes, STA tends to reconverge to its original state, which may put the network into darkness momentarily and drop packets.

However, SDN allows network engineers to predetermine multiple paths, and by design, SDN failover occurs in <100 microseconds. Network healing performance clearly favors SDN in OT networks [10]. This fast failover feature significantly increases the safety in real-time protection applications like arc-flash mitigation.

For example, assume a catastrophic situation occurs when the network link fails at the same time a trip or arc is detected. Then, assume that protection is achieved with GOOSE communications. The first packet may be lost, but the SDN device heals in less than 100 microseconds, so the next packet that is transmitted 4 milliseconds later will be received and the availability will be retained.

## VIII. IEC 61850-9-2 SV AND SDN

The IEC 61850-9-2 SV system replaces copper cables with fiber-optic links that transfer digitized data from the primary equipment in the substation yard to the control house. Primary equipment analog and control signals are connected to a merging unit (MU) (i.e., the SV publisher). The MU digitizes the analog signals at a specific sampling rate and converts them into SV streams. The streams are published to control and protective relays in the control house over a single or dual fiber-optic cable, which is dedicated only to SV and GOOSE signals. The protective relays (i.e., the SV subscribers) in the control house subscribe to these SV streams and use the information to operate their protection principle. They eventually send commands back to the MU via GOOSE to control breakers and protects the primary equipment (see Fig. 8).

SV requires an external clock signal, such as PTP or IRIG-B, to operate. PTP operates over the Ethernet network and uses the process bus or station bus to synchronize the SV devices.

An IEC 61850-9-2-compliant SV message with three-phase currents, three-phase voltages, and a 10-byte SV identifier is published at 4.8 kHz, which means an MU can sample 80 samples per cycle and 4,000 samples per second in a 50 Hz power system. One packet every 250 microseconds can consume 5.6 Mbps of bandwidth. With several streams in place, these SV messages can consume a significant part of a 100 Mbps network bandwidth.

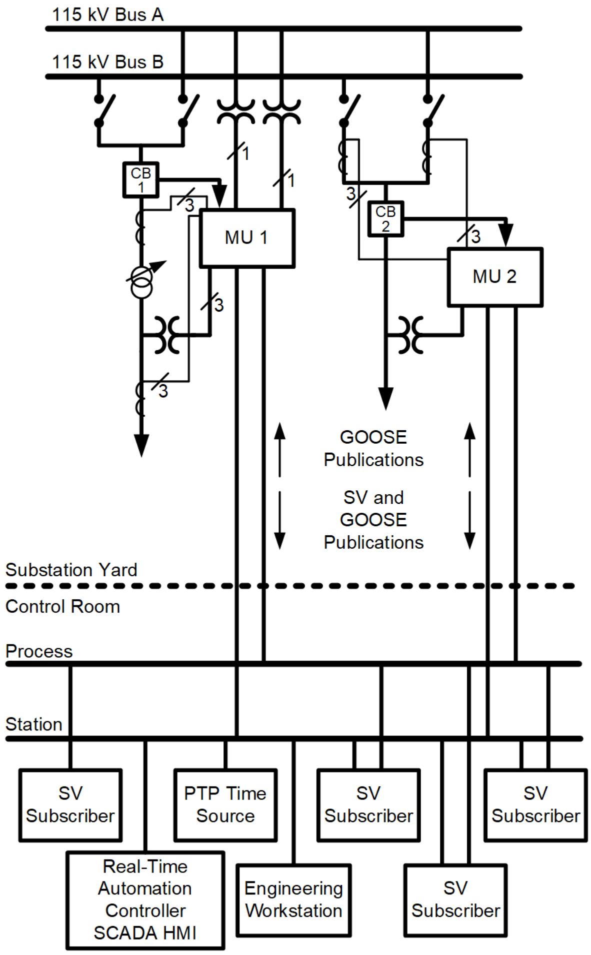


Fig. 8. Sample SDN network with logically separated station bus and process bus.

GOOSE messages are also present on the same network path. Because of their heartbeat publication rate, they can consume a large amount of bandwidth when the protection and control system experiences significant events. A faster network backbone (1 Gbps or more) can alleviate this situation. Without proper network management of the SV and GOOSE messages, the process bus network can experience a flood of traffic (e.g., ARP traffic and other broadcast traffic), causing congestion and resulting in critical data loss. Depending on the internal construction, the network can also cause processing burdens for IEDs and MUs that must process and discard traffic not intended for them [5].

OT SDN provides complete SV traffic engineering. SV flows are engineered to forward SV packets from MUs to the subscribed SV protection relays only. With its deny-by-default network design, a PTP-enabled SDN network manages SV (and GOOSE streams) reliably, with the submicrosecond time synchronization required by protection applications.

Each SV stream in SDN can be controlled to have one, two, or multiple paths to communicate with GOOSE and SV streams from the same MU and can use a different path to communicate to protective relays, which can reduce the burden in the network that their multicast heartbeat publications cause. This allows the full network bandwidth to be consumed, which is not the case with RSTP-based networks because STA logically disables part of the network to avoid network loops.

With OT SDN technology, IEC 61850 SV and GOOSE on the process bus and IEC 61850 MMS on the station bus can be deployed on the same Ethernet network by logically separating them and still keeping PCEN performance in compliance to standards.

GOOSE and SV messages can be restricted to their own logical networks while priority is applied for each flow to maintain the QoS. GOOSE, SV, and PTP traffic can be designed to have higher priority than MMS and other engineering access traffic.

With the fast failover mechanism (<100 microseconds) in SDN switches, the SV packets (which are transmitted every 250 microseconds between the MU and SV subscribers) can only be lost if they are already on the cable when the failure occurs.

Fig. 9 is an example communications network that demonstrates the failover performance. The MU publishes the IEC 61850-9-2LE SV message at 80 samples per cycle (4,000 samples per second in a 50 Hz power system or one packet every 250 microseconds).

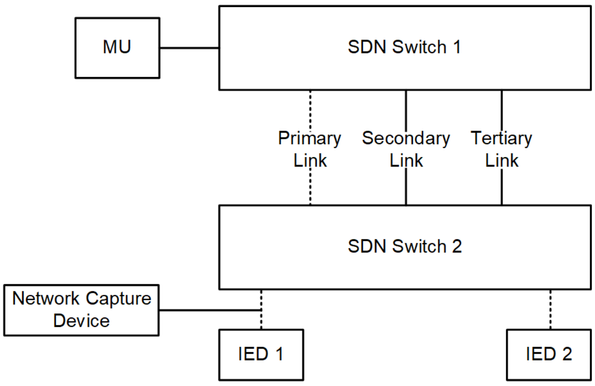
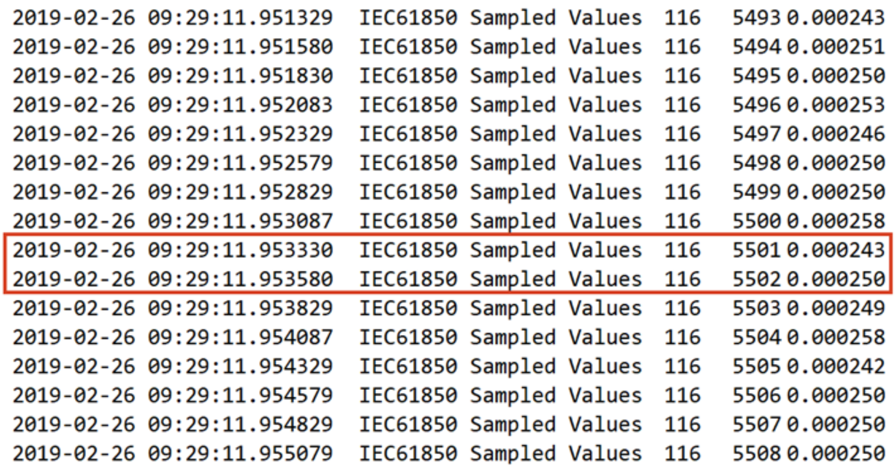


Fig. 9. Fast failover measurement example setup.

In Fig. 9, IED 1 was replaced with a network capture device to capture the SV streams. Backup paths were preprogrammed in SDN Switch 1. The primary link, which carries the SV message, was removed from SDN Switch 1. SDN Switch 1 immediately (<100 microseconds) started outputting the SV stream from the primary port to the secondary port and then to the port where IED 1 was connected.

Fig. 10 shows an event capture of the Ethernet traffic upon disconnecting the primary link from SDN Switch 1. No SV packets are lost.



```
2019-02-26 09:29:11.951329  IEC61850 Sampled Values  116   5493 0.000243
2019-02-26 09:29:11.951580  IEC61850 Sampled Values  116   5494 0.000251
2019-02-26 09:29:11.951830  IEC61850 Sampled Values  116   5495 0.000250
2019-02-26 09:29:11.952083  IEC61850 Sampled Values  116   5496 0.000253
2019-02-26 09:29:11.952329  IEC61850 Sampled Values  116   5497 0.000246
2019-02-26 09:29:11.952579  IEC61850 Sampled Values  116   5498 0.000250
2019-02-26 09:29:11.952829  IEC61850 Sampled Values  116   5499 0.000250
2019-02-26 09:29:11.953087  IEC61850 Sampled Values  116   5500 0.000258
2019-02-26 09:29:11.953330  IEC61850 Sampled Values  116   5501 0.000243
2019-02-26 09:29:11.953580  IEC61850 Sampled Values  116   5502 0.000250
2019-02-26 09:29:11.953829  IEC61850 Sampled Values  116   5503 0.000249
2019-02-26 09:29:11.954087  IEC61850 Sampled Values  116   5504 0.000258
2019-02-26 09:29:11.954329  IEC61850 Sampled Values  116   5505 0.000242
2019-02-26 09:29:11.954579  IEC61850 Sampled Values  116   5506 0.000250
2019-02-26 09:29:11.954829  IEC61850 Sampled Values  116   5507 0.000250
2019-02-26 09:29:11.955079  IEC61850 Sampled Values  116   5508 0.000250
```

Fig. 10. SV traffic event capture during failover.

## IX. Conclusion

Communications devices have become increasingly complex. This is due in part to device designs that make it necessary for intelligence be placed inside each network device. Placing more functionality into the switch hardware in some ways simplifies the network. On the other hand, it makes the devices more complicated because of the difficult handshakes and tradeoffs between handling packets in hardware versus software. In addition, the need to continuously run and manage the devices results in increased costs per device due to the processing power required to run that software as well as the storage capacity needed to hold it [1].

Any enhancement in the communications networks for critical infrastructure should start with the application requirements and improve existing reliability and security. SDN is a promising technology. It is the future of the communications network for the IT and OT industries. SDN offers more room for an engineer to design a communications network rather than depending on control plane protocols. RSTP loops and delays are a nightmare for a network engineer. SDN technology has started a new era in the communications field. No MAC address table or RSTP are required, and the self-sustainable network is engineered for business needs and application requirements. The performance difference between SDN technology and traditional Ethernet technology is immense.

SDN is not a zero-packet-loss technology. The packets can be dropped if they are on the link or in the switch when it fails. However, the <100-microsecond failover fulfills the entire application requirement in the OT network for fast trip signal transfer and digital SV streams requirements. Using SDN switches to separate the station bus and process bus reduces the number of network components and allows full use of available network bandwidth. SDN allows system owners to centrally monitor and deploy managed change control services without the risk of application disruption [4].

OT network cybersecurity requirements can be met by SDN technology, which can offer multilayer security with controlled traffic. ICS application requirements do not change day-to-day, so a perfectly engineered SDN network can provide flexibility in security and performance. This paper examines the benefits of applying SDN technology over traditional Ethernet technology to OT networks.

Traditional Ethernet networks cannot tackle OT industry challenges. The OT industry requires stringent performance, determinism, and reliability to keep the systems running in real-time environments. SDN improves system availability, scalability, security, efficiency, management, and predictive testing, and it offers better situational awareness and overall network performance.

## X. References

[1] P. Göransson, C. Black, and T. Culver, *Software Defined Networks: A Comprehensive Approach*, second edition, Morgan Kaufmann, 2016.

[2] IEEE Standard 802.1, IEEE Standard for Ethernet.

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

[4] M. Hadley, D. Nicol, and R. Smith, "Software-Defined Networking Redefines Performance for Ethernet Control Systems," proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2017.

[5] C. Gray, "How SDN Can Improve Cybersecurity in OT Networks," proceedings of the 22nd Conference of the Electric Power Supply Industry, Kuala Lumpur, Malaysia, September 2018.

[6] Cloudflare, Inc., "SYN Flood Attack," May 2019. Available: cloudflare.com/learning/ddos/syn-flood-ddos-attack/.

[7] Y. Hu, A. Yang, H. Li, Y. Sun, and L. Sun, "A Survey of Intrusion Detection on Industrial Control Systems," *International Journal of Distributed Sensor Networks*, Vol. 14, Issue 8, August 2018.

[8] S. Chelluri, D. Dolezilek, J. Dearien, and A. Kalra, "Design and Validation Practices for Ethernet Networks to Support Automation and Control Applications," proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2014.

[9] S. Chelluri, D. Dolezilek, J. Dearien, and A. Kalra, “Understanding and Validating Ethernet Networks for Mission-Critical Protection, Automation, and Control Applications,” March 2014.

[10] R. Bobba, D. R. Borries, R. Hilburn, J. Sanders, M. Hadley, and R. Smith, “Software-Defined Networking Addresses Control System Requirements,” *Sensible Cybersecurity for Power Systems: A Collection of Technical Papers Representing Modern Solutions*, 2018.

## XI. Biographies

**Anwar Habeeb Moinudeen** is a graduate of Kerala University where he received his BTech degree in information technology. Anwar joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2016 as a communications application engineer in Manama, Bahrain, where he supports communications and network-related products. Before joining SEL, Anwar worked as a network engineer for 6 years for an internet service provider.

**Ammad Ali** is an application engineer with Schweitzer Engineering Laboratories, Inc. (SEL) in the Middle East. He earned his bachelor’s degree in electronics engineering from the GIK Institute of Engineering Sciences and Technology in Pakistan. He is a member of IEEE and has 10 years of experience in the controls, automation, and communications fields. He has contributed to projects with various utilities and industrial customers in the Middle East and North Africa.

20190524 • TP6920-01