21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2018 Grid of the Future Symposium

Improve Protection Communications Network Reliability Through Software-Defined Process Bus

Q. YANG, R. SMITH
Schweitzer Engineering Laboratories, Inc.
USA

SUMMARY

In an IEC 61850 digital substation, merging units connected to instrument transformers stream analog measurements as data packets via an Ethernet network. These data packets are used for power system protection and control. However, the added merging units and Ethernet switches increase the possible points of failure in the protection system and reduce the system availability.

To minimize single points of failure and improve the availability of a protection system composed of relays and merging units, this paper proposes applying software-defined networking (SDN) path programming and fast failover features to achieve Sampled Values (SV) stream redundancy. This method achieves redundancy by dynamically substituting a missing or problematic SV stream with a good SV stream. This method can be implemented on SV relays or Ethernet switches. This makes it possible for system designers to improve the availability of instrument transformer measurements and create redundancy for power system protection without adding new current or voltage transformers.

IEC 61850-based protection communications networks include time-critical traffic (e.g., SV and GOOSE messaging on the process bus) and other traffic, such as manufacturing message specification (MMS) and engineering access on the station bus. This paper also discusses using SDN to manage an IEC 61850 network by logically separating station bus and process bus traffic using SDN path programming. This approach increases cybersecurity, protects the quality of service of time-critical traffic delivery, and provides greater network situational awareness.

KEYWORDS

Sampled Values, software-defined networking, process bus, reliability, redundancy.

qiaoyin_yang@selinc.com

1 INTRODUCTION

Traditional network switches depend on proprietary firmware to configure packet routing. The static network architecture formed by these switches is difficult to adapt as the network grows or applications change. Managing a fast-growing network demands agility and intelligence. A new network architecture approach, software-defined networking (SDN), decouples the network management functionality from the switch hardware and places it into a centralized controller known as the control plane. In SDN, network engineers can create network traffic forwarding rules for a fleet of switches in the control plane software. The switches then execute the rules received from the control plane to forward traffic as configured. The switches in this architecture are simpler with the control plane removed, which results in less patch management and fewer errors.

SDN was first used in the information technology (IT) industry for applications such as data center networks and software-defined wide-area networking. However, the SDN architecture and its many features (e.g., network traffic programmability and network statistics) can provide innovative solutions to networking challenges in other industries.

Operational technology (OT) SDN does not change the basic architecture of SDN but is rather a way of applying SDN to solve unique challenges in automation networks composed of devices such as switches and programmable logic controllers. Such networks are often used for industrial control systems, which focus on reliability, security, and real-time performance. Table 1 shows a summary of how SDN is applied to an OT network versus an IT network [1]. Features of OT SDN, such as deny-by-default network access, bring security to substation networking. Purpose-engineered networking and fast healing provide new opportunities to innovate substation automation solutions.

Table 1 OT SDN vs. IT SDN

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

In industrial control systems using SDN, all communications to and from each device are purpose-engineered. To achieve reliability, redundant (primary and failover) network flows can be proactively engineered to achieve the predictable and repeatable behavior desired for such systems.

This paper discusses applying OT SDN technology to an IEC 61850 communications network. Purpose-engineered network control creates a confined Sampled Values (SV) network and reduces unintended network bandwidth consumption. In addition, the paper describes the SDN fast-failover function in SV communications and its possible application to IEC 61850 networks.

The applications and examples described use the OpenFlow® 1.3 protocol to communicate between the control plane software and the SDN switches, and they use the top-level SDN architecture shown in Figure 1.

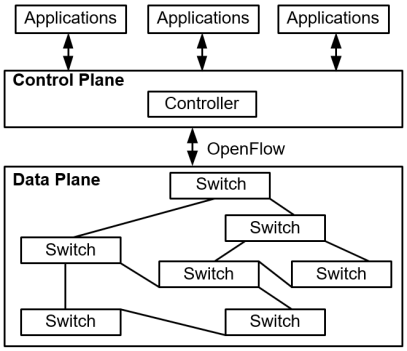


Figure 1 SDN Architecture Overview

2 IEC 61850-BASED SUBSTATION PROTECTION COMMUNICATIONS NETWORKS

Ethernet-based substation protection and control systems (such as IEC 61850 process bus networks) must be fast, deterministic, and reliable [2]. IEC 61850 [3] details a communications architecture for substation automation systems. The station bus network is the communications channel between the control house equipment and the IEDs at the bay level, as shown in Figure 2. Such communications networks typically carry manufacturing message specification (MMS), GOOSE, synchrophasor (intersubstation GOOSE and SV), and other types of engineering access communications. The station bus network is also typically used for exchanging data between SCADA systems and IEDs.

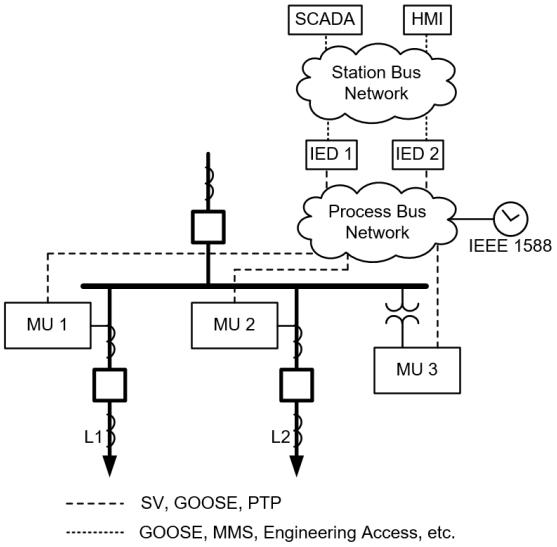


Figure 2 Physically Separated Station Bus and Process Bus

The process bus network is the communications channel between the bay-level IEDs and the merging units (MUs) in the yard. It is designed to exchange time-critical data. This communications network usually carries SV, GOOSE, and IEEE 1588 [4] Precision Time Protocol (PTP) messages. A merging unit samples and digitizes analog signals. These samples are then encoded as Ethernet frames and published into the process bus at a fixed rate in a multicast fashion. An IEC 61850-9-2LE-compliant SV message with 3 phase currents, 3 phase voltages, and an SV identifier of 10 bytes, published at 4.8 kHz, consumes 5.6 Mbps of bandwidth. With several streams in place, these SV messages can consume a significant part of a 100 Mbps network bandwidth. 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. This situation can be alleviated by using a faster network backbone (1 Gbps or more).

Without proper network management of the SV and GOOSE messages, the process bus network can experience floods of traffic and network congestion, resulting in message losses. Depending on the internal construction, the network can also cause processing burdens for IEDs and merging units that have to process and discard traffic not intended for them.

In an OT SDN network, traffic is purpose-engineered such that the messages are forwarded only when they match carefully configured criteria. SDN technology allows the deployment of a unified IEC 61850 communications networks in which the process bus and station bus traffic are logically separated and managed as shown in Figure 3.

Multicast traffic, such as GOOSE and SV messages, can be confined in its own logical network while quality of service is applied to manage the priorities of different types of traffic. A good rule is to assign the highest priority to SV, GOOSE, and PTP traffic, which most protection and control applications depend on. A medium priority should be assigned to MMS and GOOSE traffic that serves SCADA and HMIs, and a low priority should be used for engineering access communications.

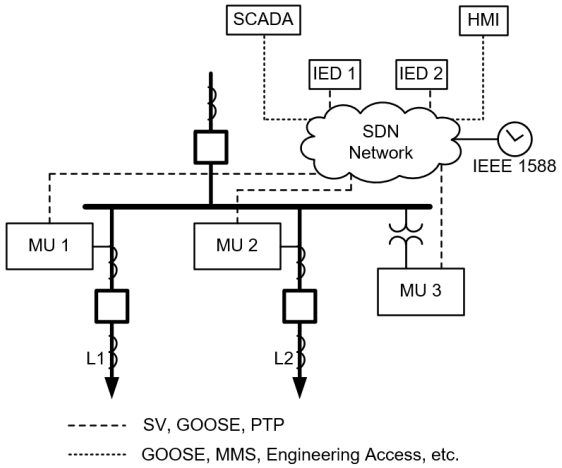


Figure 3 Unified SDN Network With Logically Separated Station Bus and Process Bus

3 SOFTWARE-DEFINED PROCESS BUS

Regardless of the communications architecture of the station bus and process bus, SDN technology provides an improved method to partition and control virtual networks for different types of traffic as compared with VLANs, which tag Ethernet messages with VLAN identifiers and priorities to determine message routing.

In an SDN network, the control plane software manages a fleet of SDN switches. The software detects the topology of the switches, supports traffic engineering, and provides network status monitoring.

SDN traffic engineering includes three steps. The first is to define match criteria for incoming packets. The criteria packets are matched against the ingress port, Ethernet source or destination MAC address, Ethertype, VLAN identifier, IP source or destination address, and so on. The second step is to define actions for ingressing messages that match the various criteria. The last step is to define a set of counters that can be used to monitor the ingress and egress of traffic and the overall network health.

With SDN, process bus traffic is defined with engineered paths regardless of the type of message (unicast or multicast). This paper uses the term “software-defined process bus” to describe a network bounded by these engineered paths, which can be freely configured to support the different network topologies required to meet design constraints or individual device capabilities.

In an IEC 61850 communications network, GOOSE and SV publisher and subscriber relationships are determined by application and described using Substation Configuration Language (SCL) files. Template-based network path programming can enable substation network engineers to design SDN networks at the power system application level (using IEC 61850 configuration tools) instead of defining match and forward rules based on individual Ethernet message types. Statistics that detail the

number of packets transmitted and received per application (e.g., SV publication) can be provided as a template for network monitoring.

4 IMPROVING COMMUNICATIONS SYSTEM RELIABILITY USING SDN

Native features of SDN technology have inspired new solutions to the challenges of substation protection and control networks (e.g., IEC 61850 substation network automation). SDN decouples the switch configurations from the switch hardware. This reduces the processing burden on the switches and leaves more processing power to improve reliability and performance.

The control plane, by centralizing the control and monitoring of the entire fleet of network switches, can reduce operational expenses. A fleet of switches can be managed as a single asset, and engineers do not need physical access to switches to make configuration changes.

OT SDN switches support deny-by-default network access control and centralized monitoring of the network health. The monitored statistics may include the number of packets or bytes received or transmitted per port and the number of packets or bytes received per engineered path.

In an SDN network, all network paths must be preprogrammed, including failover paths. Path planning brings determinism and reliability to the substation protection communications network. Aside from these obvious advantages, logical path programming and fast failover for faulted network connections provide opportunities to improve the reliability of the protection communications network.

5 EXISTING METHODS FOR NETWORK HEALING AND REDUNDANT NETWORKING

Common methods for increasing the reliability of a protection communications network include automated network healing (e.g., Rapid Spanning Tree Protocol [RSTP]), redundancy protocols (e.g., Parallel Redundancy Protocol [PRP] and High-Availability Seamless Redundancy [HSR] protocol), and physically adding redundant network devices and cables. The fast failover and preprogrammed network paths of SDN can improve these methods by minimizing communications interruptions and improving the availability and reliability of the protection communications network upon faulted network conditions.

When a faulted network condition occurs, RSTP can heal the network by finding a new path to deliver the packets to their destination. RSTP ensures that there is only one active path between the source and destination at any time, and when there are topology changes (caused by a link failure, for example) it discovers a new path. RSTP is a healing technology, not a redundancy technology. This means that, upon faulted network conditions, packets can be dropped during network reconfiguration and link restoration. The speed of RSTP network link recovery is in the range of dozens to hundreds of milliseconds, which can result in hundreds of lost SV messages and a temporary loss of associated protection functions.

Two common methods for providing network redundancy are PRP and HSR protocol. PRP creates parallel paths through redundant networks that duplicate SV packets travel on. Losing one path has no impact on the parallel path. PRP uses a 6-byte packet trailer that can be ignored by non-PRP nodes and which is also backward-compatible with standard Ethernet network hardware.

Unlike PRP, HSR does not use a standard Ethernet frame and requires devices to be in a ring topology so that redundant messages can be sent around the ring in both directions. Messages travel through all devices in the ring, and each device on the HSR ring must process or forward the message. This increases processing burden and network latency while limiting the maximum number of devices on the ring. The sending device is responsible for removing the circulating packets from the ring to prevent infinite packet circulation.

In both PRP and HSR topologies (see Figure 4 and Figure 5), the receiver receives duplicate messages; it processes the packet that arrives first and discards the duplicate. Both methods provide dual-network redundancy. However, network equipment, such as merging units and relays, must support PRP or

HSR. Both PRP and HSR only provide redundant network paths and leave other tasks such as multicast grooming to network engineers.

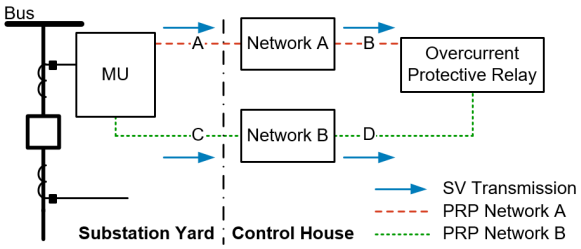


Figure 4 Network Redundancy With a PRP Network

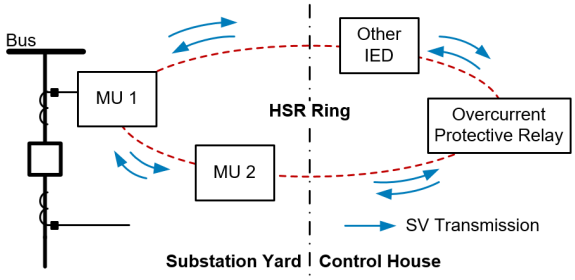


Figure 5 Network Redundancy With an HSR Network

6 APPLYING SDN TO IMPROVE INSTRUMENT TRANSFORMER SIGNAL AVAILABILITY AND RELIABILITY

In an IEC 61850 process bus, advanced applications of SDN fast failover and path programming functions can provide instrument transformer measurement redundancy by rerouting and sharing SV streams through an SDN network.

6.1 Using SDN to Improve PRP Network Reliability

The fast failover feature of SDN can enhance the availability of a PRP network. Figure 6 shows a PRP application using two SDN switches with a failover path between them.

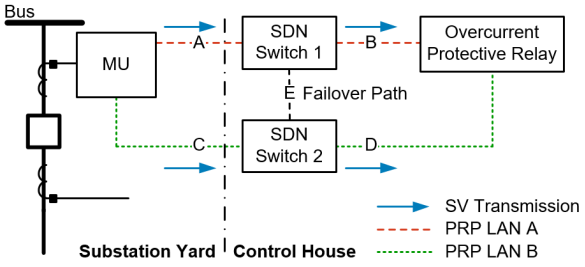


Figure 6 PRP Network With SDN Switches

If Paths B and C fail, for example, the PRP network would not be able to deliver the SV messages from the merging unit to the relay. However, with the SDN fast failover function, the SV messages can travel through Path A, then Path E, then Path D to the relay. Some SDN networks provide a fast failover time of less than 100 µs for any link or switch failure, regardless of the architecture of the network, improving the reliability of the protection communications PRP network.

6.2 Creating a Parallel Redundancy Network Using SDN Path Programming

With the network programmability of SDN, it is possible to create parallel redundancy without the use of the PRP protocol or the need to append PRP trailers to the SV message.

SDN technology can be integrated into IEDs, as shown in Figure 7. In such networks, the SDN module on the merging unit duplicates the SV stream and sends it out from two Ethernet ports. These two SV streams travel on two independent LANs and arrive at the relay SDN module. The relay SDN module

determines that Path G is the primary path. It forwards the SV stream on Path B to Path G for the relay to process, and it does not forward the SV messages on Path D unless it detects a network issue on its primary path. SDN system counters can be deployed to easily monitor delivered messages.

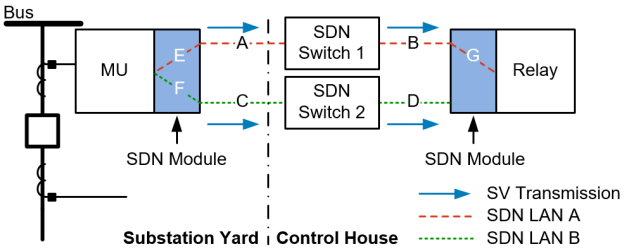


Figure 7 Parallel Redundancy Created Using SDN Path Planning

The main advantage of the SDN approach is the ability to decouple the network configuration from the switch hardware and to move it into the control plane software. It is possible to manage all the network configurations, including those of IEDs, using the SDN control plane software. If implemented correctly, the proposed approach can significantly improve the efficiency of managing substation network configurations and give network engineers new tools to design, manage, and maintain the substation network.

6.3 Applying SDN to Improve Instrument Transformer Signal Availability Via Data Sharing

SDN can provide instrument transformer signal redundancy over a network. In IEC 61850-based substations, instrument transformer signals are digitized and published as multicast messages on a network. IEDs subscribe to one or more streams of these SV messages. Section 6 provides an example of applying SDN to create logical network paths that share SV streams representing the same VT or CT measurements to provide redundant measurements to IEDs. An SDN network can be configured as a mesh-ring topology or a PRP network. The IEDs run a program to determine the active SV stream subscription. Another approach is to program the SDN network to route the redundant SV stream to the IED for issues such as broken Ethernet fibers and switch failures.

6.3.1 Supplying Redundant CT and VT Signals Via SV Subscription Switching at IEDs

Figure 8 shows an example of switching VT signals at an IED. The busbar has *n* feeder lines, each protected by a distance protection IED. To improve reliability, the system is designed with two VTs. The first group of feeders, Lines 1 to 10, are protected using the voltage signal from VT 1. The second group of feeders, Lines 11 to *n*, are protected using the voltage signal from VT 2. In traditional substations that use copper wiring for secondary circuits, a single VT would typically be used. If VT redundancy is desired, the VT 2 signal needs to be wired to each IED, which may be physically prohibitive for a large bus.

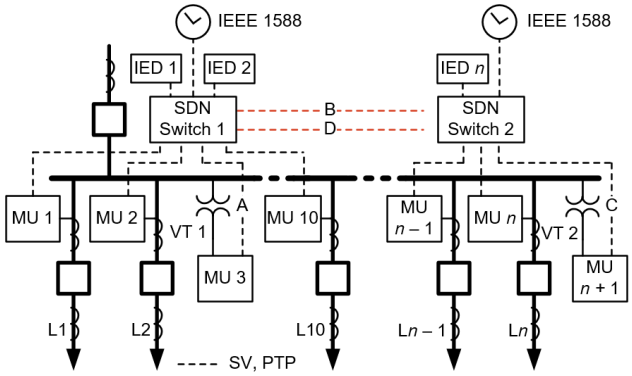


Figure 8 Sharing VT Measurements Between Feeder Line Protection Systems

With SDN path programming and fast failover, primary and backup Paths B and D can be added and logical paths can be programmed between the two SDN switches. Paths B and D serve as primary and backup paths to pass the SV messages from MU *n* + 1 to all the IEDs in the first group. Similarly, the SV messages from MU 3 are passed to the second group of feeder relays. The relays subscribe to both

SV streams such that the VT 1 and VT 2 measurements are available at all times. Such relays can be programmed to switch from one VT signal to the other if they detect a loss of the primary VT measurements. With the application of a backup link (Path D) between the two SDN switches, the reliability between the two SDN switches is improved. The failover from Path B to Path D can occur in less than 100 µs.

In addition to using SDN network path programming and fast failover to improve instrument transformer signal reliability, the network can be replicated to form a PRP network to provide full network communications path redundancy. This type of sharing is especially valuable for medium-voltage applications where conventional VTs may be replaced with low-energy voltage dividers whose output cannot drive multiple relays. In such systems, relays are typically mounted in the immediate vicinity of the breakers, with the merging unit functionality integrated into the relay.

6.3.2 Supplying Redundant CT/VT Signals Via Network Level Switching

To limit bandwidth usage and reduce the processing burden on IEDs, another approach to supplying redundant instrument transformer signals via SDN is to preprogram failover logical network paths to handle faulted network conditions. That is, upon the loss of an SV stream, an SDN network can be programmed to route SV messages that contain the same measurements to the IEDs via these preprogrammed logical paths and thus maintain protection without interruptions.

An IEC 61850 9-2LE-compliant [5] SV publication has a transmission rate of 4.8 kHz for a 60 Hz power system and 4 kHz for a 50 Hz power system. This converts to sample transmission intervals of 208 µs and 250 µs, respectively. Networks with a fast failover of <100 µs cause no more than one sample to be lost in this scenario. If an SV IED is designed to tolerate a missing or out-of-sequence SV message, the loss of this one sample will have no impact. Thus, SDN provides a platform to accomplish SV stream switching without interrupting protection.

Traditional networking using RSTP only heals networks for the destination. This means that when packets enter the network, RSTP discovers and applies one forwarding path for every source and destination pairing. SDN provides the same destination healing as RSTP but also provides source redundancy. For example, as long as the primary SV stream continues to arrive at the SDN switch, the switch can be programmed not to forward the SV packets from the backup stream. However, when the SV packets from the primary source are no longer detected, the SV packets from the backup source can be delivered to the destination instead. This cutover is, again, accomplished in less than 100 µs. Dynamically switching to preprogrammed network paths in SDN switches makes it possible to share VT and CT information within a substation network without requiring an IED to subscribe to two SV streams. Since the substitution is seamless, IEDs must be able to detect the change and perform the necessary supervision of the local protection functions. Detection can be accomplished by monitoring the SV stream source MAC address in combination with the sample synchronization flag.

SDN allows SV streams that originate from instrument transformers that measure the same voltages or currents in a substation to be shared. Advanced applications of this dynamic switching can be extended to a system that does not have truly redundant instrument transformers. For example, a protection system is divided into different protection zones, and each zone overlaps with adjacent zones. VT measurements on the same bus or a bus tied with a tie breaker are the same under most circumstances. Dual CTs on the same side of a breaker have the same current magnitude and phase angle. To avoid blind spots in the power protection system, an inboard and an outboard CT with a common breaker are often used to protect two zones that overlap. These CT magnitude measurements in an overlapped protection zone that shares a common breaker are the same and typically have opposite polarities (depending on the CT configuration).

For these physical VT and CT arrangements, the published SV streams that represent CT or VT measurements are available on an Ethernet network. Upon faulted network conditions, such as a broken fiber-optic cable or a failed network switch, preprogrammed logical network paths can be used to supply protective relays with the same current or voltage measurements but from another merging unit.

Therefore, signal redundancy can be achieved upon network faulted conditions. The failover from the active logical path to the failover path takes less than 100 µs, as demonstrated later in this paper.

Although not applicable for all applications (e.g., loss of protection zone overlap) and dependent on close matching of the independent merging unit measurements, network-based stream substitution aided by custom-built protection logic can be useful in emergency situations.

An example application of this scheme is shown in Figure 9. The line-side CT and the bus-side CT provide the same current information. These CTs are connected to merging units. SV messages from MU 1 are programmed to travel through SDN Switch 1 to the SV Distance Relay. SV messages from MU 2 are programmed to travel through SDN Switch 2 to the SV Bus Relay. SV messages can travel from MU 1 to SDN Switch 2 via Path C or Path D. The SV messages are not forwarded until a monitored condition occurs.

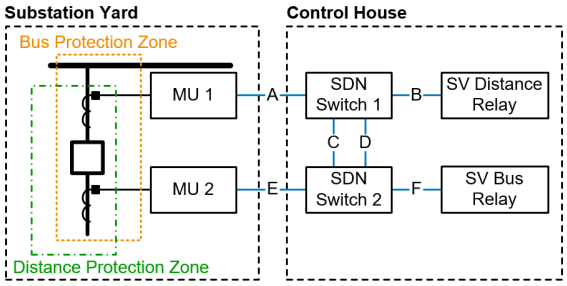


Figure 9 Bus-Side and Line-Side CTs Measuring the Same Current When the Breaker Is Closed

In this example, if a fiber-optic cable breaks between MU 2 and SDN Switch 2, SDN Switch 2 detects the link loss and starts forwarding the SV messages from MU 1 to the SV Bus Relay. With this preprogrammed failover network path, SV messages containing the same measurements are sent to the bus relay. The bus relay protection continues to operate with substituted current measurements. The fast failover speed of <100 µs may still cause a sample loss for an SV stream published at a constant 4.8 kHz, which can affect the IED operation if the number of samples lost exceeds the number that the IED can tolerate.

The polarities of the two CTs shown in Figure 9 are the same. If the polarities of the two CTs are different (as in a typical protection application), the SV relays must be able to detect that an SV stream has been substituted and apply the correct polarity to the incoming current before using it for protection.

7 INSTRUMENT TRANSFORMER SIGNAL SUBSTITUTION EXAMPLE

Figure 10 shows a test setup used to demonstrate the data substitution example described in Figure 8. In this example, the SV stream from MU 3 takes Path A and Logical Path E to IED 1. The SV stream from MU 21 travels on Logical Path M and Path B to SDN Switch 1. This SV stream is not forwarded to IED 1. However, if Path A between the SDN Switch 1 and MU 3 fails, the loss of this link is detected by SDN Switch 1, which immediately starts forwarding the SV stream coming from SDN Switch 2 to IED 1 via Logical Path F.

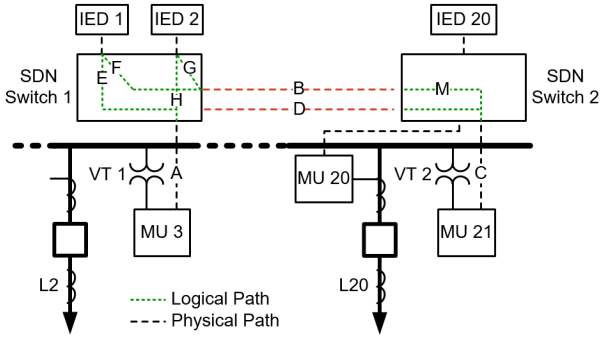


Figure 10 Redundant Voltage Measurement Substitution Example Setup

To demonstrate the redundancy performance, the authors set up a network with the configuration shown in Figure 11. IED 1 was removed to connect a network capture device to capture the switching of the SV streams. MU 3 (VT 1) was disconnected from SDN Switch 1. Software-defined logical paths were preprogrammed to pass the MU 21 (VT 2) SV stream to the port where IED 1 was connected to SDN Switch 1. SDN Switch 1 immediately (<100 µs) started outputting the SV stream from MU 21 to the port where IED 1 was connected.

Figure 12 shows a network capture of the Ethernet traffic upon disconnecting MU 3 from SDN Switch 1. The network traffic was captured using a tool that is capable of time-stamping Ethernet messages with ±100 ns accuracy. This captured network traffic was then decoded using Wireshark® software.

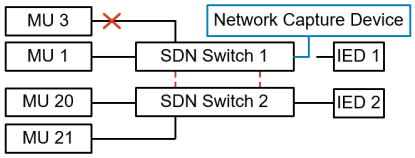
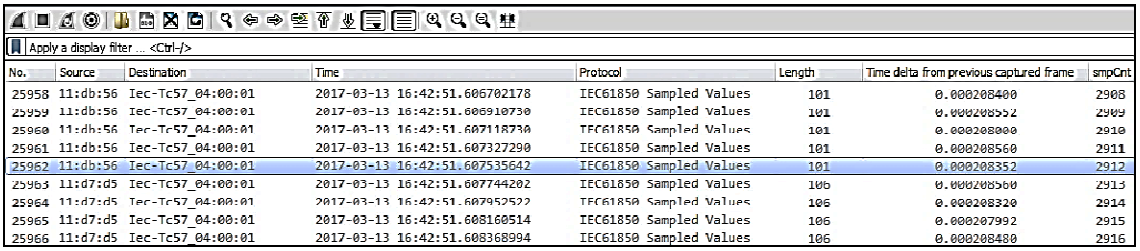


Figure 11 Process Bus Traffic Capture Diagram


Apply a display filter ... <Ctrl-/>

No.	Source	Destination	Time	Protocol	Length	Time delta from previous captured frame	smpCnt
25958	11:db:56	Iec-Tc57_04:00:01	2017-03-13 16:42:51.606702178	IEC61850 Sampled Values	101	0.000208400	2908
25959	11:db:56	Iec-Tc57_04:00:01	2017-03-13 16:42:51.606910730	IEC61850 Sampled Values	101	0.000208552	2909
25960	11:db:56	Iec-Tc57_04:00:01	2017-03-13 16:42:51.607118730	IEC61850 Sampled Values	101	0.000208000	2910
25961	11:db:56	Iec-Tc57_04:00:01	2017-03-13 16:42:51.607327290	IEC61850 Sampled Values	101	0.000208560	2911
25962	11:db:56	Iec-Tc57_04:00:01	2017-03-13 16:42:51.607535642	IEC61850 Sampled Values	101	0.000208352	2912
25963	11:d7:d5	Iec-Tc57_04:00:01	2017-03-13 16:42:51.607744202	IEC61850 Sampled Values	106	0.000208560	2913
25964	11:d7:d5	Iec-Tc57_04:00:01	2017-03-13 16:42:51.607952522	IEC61850 Sampled Values	106	0.000208320	2914
25965	11:d7:d5	Iec-Tc57_04:00:01	2017-03-13 16:42:51.608160514	IEC61850 Sampled Values	106	0.000207992	2915
25966	11:d7:d5	Iec-Tc57_04:00:01	2017-03-13 16:42:51.608368994	IEC61850 Sampled Values	106	0.000208480	2916

Figure 12 Decoded SV Traffic

Figure 12 shows that the SDN switch starts outputting an SV stream from a different source MAC address at time 16:42:51.607744202. The last two octets of Packet 25962, from MU 3, are db:56 in the source MAC address. The last two octets of Packet 25963, from MU 21, are d7:d5 in the source MAC address. Packet 25962 and Packet 25963 have a time change from the previously captured frame of 208 µs. The sample count is continuous, from 2912 to 2913. In this example, the engineered SDN network substituted the missing SV stream seamlessly.

Figure 13 shows the analog signals seen by the network traffic capture tool where IED 1 was connected.

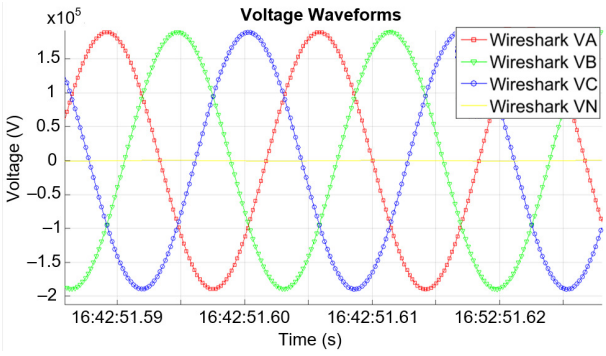


Figure 13 Sinusoidal Signals Continuing as SDN Creates a New Logical Path

To observe the signal, the authors created a software tool to display the signals from the captured network traffic. At time 16:42:51.60, there is no discontinuity of the analog signals. The SDN preprogrammed path for fast failover successfully provided a redundant SV stream to IED 1 and the protection was not compromised. Signal redundancy for protection was accomplished without adding another VT or merging unit.

CONCLUSION

New Ethernet technology provides opportunities to improve the reliability of protection and control communications networks and innovate communications schemes. SDN allows OT network engineers to purpose-engineer their networks to support even the most demanding applications to operate, control, and monitor critical infrastructure. It allows system owners to centrally monitor and deploy managed change-control services without the risk of application disruption.

IEC 61850 promotes protection and control schemes based on Ethernet communication. However, Ethernet-based process bus technology must be reliable and robust because a majority of protection and control applications depend on it.

SDN technology provides a new network engineering platform capable of solving many unique challenges in the protection communications network. The path programming function and fast failover features of SDN offer new approaches to achieve instrument transformer signal redundancy by sharing SV streams inside an SDN network. This approach can also be applied to any other process bus that is similar to those defined by IEC 61850-9-2.

Advanced applications that substitute an SV stream with another SV stream can improve communications system reliability and improve the availability of instrument transformer signals by sharing them within the SDN network.

BIBLIOGRAPHY

[1] R. Hill and R. Smith, "Purpose-Engineered, Active-Defense Cybersecurity for Industrial Control Systems," August 2017. Available: https://www.selinc.com.

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

[3] IEC 61850-7-2, Communication Networks and Systems for Power Utility Automation – Part 7-2: Basic Information and Communication Structure – Abstract Communication Service Interface (ACSI), 2010.

[4] IEEE Standard 1588-2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.

[5] UCA International Users Group, "Implementation Guideline for Digital Interface to Instrument Transformers Using IEC 61850-9-2," July 2004. Available: http://iec61850.ucaiug.org/Implementation%20Guidelines/DigIF_spec_9-2LE_R2-1_040707-CB.pdf.

20180126 • TP6805