Case Study: Implementing a Zero-Touch Deployment Methodology Using SDN to Improve the Security, Reliability, and Engineering of Substation Automation Systems in Slovenia

Darko Bordon
ELES, d.o.o.

Robert Meine, Sagar Dayabhai, and Jason Dearien
Schweitzer Engineering Laboratories, Inc.

Presented at the
PAC World Conference 2023
Glasgow, United Kingdom
June 26–29, 2023

Case Study: Implementing a Zero-Touch Deployment Methodology Using SDN to Improve the Security, Reliability, and Engineering of Substation Automation Systems in Slovenia

Darko Bordon, *ELES, d.o.o.*
Robert Meine, Sagar Dayabhai, and Jason Dearien, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Modern substation automation systems are equipped with the intelligence to detect, identify, and manage power system faults, events, and disturbances, and adjust the grid accordingly. For utilities to implement these technologies and use their benefits to move towards a digital substation, a reliable and secure communications operational technology (OT) network supporting high-speed data transfer is required. Consequently, the use of Ethernet networks has now become a critical component for power system protection and control applications. This has led to an increase in the number of network switches used in the power system over the past decade as the number of intelligent electronic devices (IEDs), applications, and data available continue to grow.**

SDN can be deployed as a solution in OT networks to address the challenges presented by traditional Ethernet networks. This paper presents a case study based on a real-world implementation that uses SDN in a modern substation automation system based on IEC 61850 at the ELES TSO in Slovenia. This case study combines the use of SDN with a zero-touch deployment (ZTD) methodology to present an innovative, application-focused engineering approach to design and secure OT networks in a substation. The advantages and disadvantages of this implementation are documented in this case study. It covers what worked well and the challenges encountered during the design, commissioning, and maintenance phases of the substation.

I. Introduction

The use of modern intelligent electronic devices (IEDs) has increased the level of integration and information that exists in a substation automation system. These IEDs and applications enable utilities like ELES to operate the power system more economically and safely, improve efficiency, and increase grid availability and reliability. They further facilitate long-term operation and maintenance, improve system restoration times, enable rapid diagnosis, and prompt notification of alarms and events of abnormalities in the power system.

For many utilities, the deployment of large communication networks to facilitate substation automation systems has introduced many challenges relating to security and technology management. Rapid Spanning Tree Protocol (RSTP)-based managed switch standards are also not designed to meet the performance and reliability requirements that are essential for the power system. Plug-and-play, best-effort solutions just won't do in the domain of critical infrastructure.

Configuring networking devices with the correct settings based on an efficient, scalable, and secure design can be a lengthy process that demands high labor costs and resources. Moreover, the power system is an appealing target for cyber attacks, so modern operational technology (OT) Ethernet networks must be designed with security in mind to protect against cyber threats. Compromise of these networks can result in widespread outages, damage to equipment, and harm to personnel. These challenges are further exacerbated for larger substations and when considering intersubstation communications for protection and control applications.

This paper explores the benefits of OT software-defined networking (SDN) and how this solution can be used to meet the stringent requirements of OT networks. Through a real-world case study, this paper further covers several challenges facing utilities with implementing a secure OT network for substation automation systems and suggests a zero-touch deployment (ZTD) approach to designing a secure network with repeatable and predictable behavior. This approach increases cybersecurity, leverages common elements in the information technology and OT space (e.g., use of IP/Multiprotocol Label Switching (MPLS) network) while maintaining a balance in their convergence, reduces engineering and commissioning costs, and improves network management and situational awareness.

II. Background

Prior research into the development trends in communication, protection, and control equipment by the secondary system department at the ELES Transmission System Operator has led to the development of a stable, available, secure, and more reliable transmission system in Slovenia.

This case study stems from the construction of a new 400/110 kV substation and new 400 kV power lines to Hungary and Croatia by the ELES Transmission System Operator (TSO) from 2018 to 2022. This construction was also the reason for the introduction of new concepts and technologies in the field of secondary systems. Subsequently, it became necessary to take a new step in the field of communications relating to secondary systems as concepts and associated technologies in the energy sector kept evolving and being regularly updated.

The decision to use the IEC 61850-based GOOSE communication protocol for a new substation for purposes of

interlocking and for teleprotection required not only a reliable and available network promoting high-speed data transfer, but also a resilient and cybersecure network. This requirement necessitated several innovative decisions to be taken during the design stage of the building of the new substation.

The first decision was to build a communications network for the IEC 61850 station bus. The chosen topology for the station bus was to use the Parallel Redundancy Protocol (PRP) based on the IEC 62439-3:2016 standard [1]. Several reasons necessitated this approach. Full redundancy not only enables reliable communication but also has advantages during substation maintenance and when performing network upgrades as it achieves uninterrupted performance for all communications within the IEC 61850 station bus.

ELES has considerable experience with using GOOSE, particularly when applying the protocol with bay computers. Therefore, the second decision was to use GOOSE communications for protection purposes; both for sending trip commands and for carrier send/receive signals between substations (as described in the case study below). This would also eliminate the need for teleprotection devices to send the signals via the ELES SDH or MPLS network.

The third decision was based on the rigorous testing of the OT SDN technology for network switches, which began in 2016. It became apparent that the introduction of SDN technology required a completely new approach to network engineering. During the testing phase, it was observed that the SDN technology increased the cybersecurity, network reliability and availability of the system and proved to be an excellent secure solution for exchanging data between substations. The use and trust of SDN technology by ELES led to the fourth decision which involved using the newly developed IEC 61850 station bus and a next generation firewall to provision remote access for protection and control. This eliminated the need for a dedicated network for remote access to protection and control devices.

III. SDN

There is a consistent increase in the use of SDN technology by TSOs globally for their critical infrastructure installations. These installations use very static configurations for devices and expect consistent, and high-performance machine-to-machine communications to perform high-speed data transfer for mission-critical protection schemes. Many of these schemes must operate reliably, even during a network failure event, in less than 3 ms as defined in IEC 61850-5 [2].

RSTP-based managed switch technology is not appropriate for critical OT networks. First, it is built on trust to allow devices to easily communicate with each other by automatically changing the data plane used by the network to move packets based on untrusted and dynamic network traffic. This behavior leaves the network and the connected devices susceptible to many security and performance vulnerabilities including Address Resolution Protocol (ARP) poisoning, MAC spoofing, and denial of service attacks. Second, traditional networks often use very slow recovery mechanisms, like RSTP, that heal the network in case of a device or link failure. The time needed for the network to recover varies greatly, anywhere from 10 milliseconds to 30 seconds, based on the topology of the network and the amount of traffic. During these reconvergence events, large amounts of traffic can be dropped, resulting in loss of communication or traffic can be duplicated causing out-of-sequence messages that can disable protection.

The use of OT SDN mitigates these challenges by providing a completely deny-by-default data plane that moves packets based on proactive traffic-engineered redundant circuit provisioning, or what SDN calls “flows.” These flows are pre-engineered based on the desired communications between different devices on the network and are optimized to move the traffic as quickly as possible based on the priority of the message, and, in the event of a network failure, automatically deliver the packets through an alternative network path without lengthy reconvergence algorithms. The advantages are possible because the OT SDN technology uses a match-then-action methodology that can identify the signature of an Ethernet packet and send it to the correct destination based on predetermined rules. This means there are no dynamic learning algorithms that can be manipulated for nefarious network attacks or reconnaissance. OT SDN only moves packets based on predefined rules which means it is inherently deny-by-default. Because the paths the traffic takes through the network are computed at design time it is also possible to precompute the failure paths so in the event of a cable or switch failure, the path the traffic should take is already known which reduces the recovery time to less than 100 µs in some commercially available OT SDN switches.

SDN decouples the network management and switch configuration functionality from the switch hardware and places it into a centralized SDN controller known as the control plane. This reduces the processing burden on the switches and leaves more processing to improve reliability and performance. This decoupling allows the SDN switches to be centrally managed which present several benefits which include:

- No physical access is required to the switches to make the configuration changes.
- End-to-end circuit provisioning is possible for service and application delivery between devices irrespective of the size of the network or topology. The SDN controller is responsible for the network configuration and will automatically provision the required end-to-end circuits and configure the SDN switches.
- Centralized management and situational awareness using the SDN controller provides complete visibility of all substation OT networks.
- SDN switches can operate autonomously without the SDN controller after the configuration is applied.

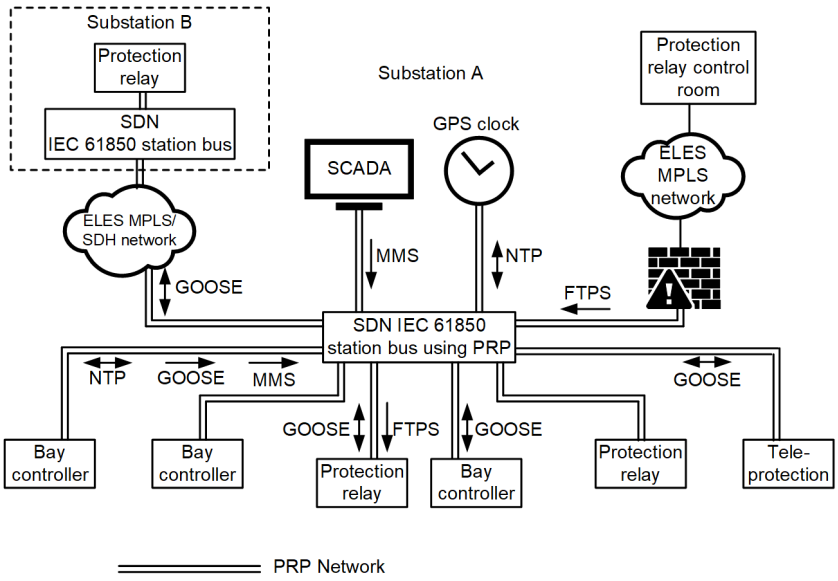

Figure 1 Network architecture of ELES substation.

IV. Case Study

Figure 1 describes the network architecture of the newly constructed substation built by ELES.

The setup of the SDN technology required the assistance of SDN network specialists because it demanded new aspects and principles of network construction. Three basic questions had to be answered which were:

1. How many devices will communicate on the new substation network?
2. What communications and data flow exist between the devices in the substation?
3. What Class of Service (CoS) regime can be applied on the network?

In addition to the IEC 61850 station bus, the design included the use of a separate single attached node (SAN) network for IEDs such as power quality and tariff meters, Phasor Measurement Units (PMUs), transformer monitoring devices, and reactor switching devices.

A. Substation IEDs

The substation included 25 bay computers, 70 multivendor IEDs, three voltage regulators, three synchronous transformer and reactor switching devices, 16 teleprotection devices, one Traveling Wave Fault Location Monitor, two substation automaton and control center gateway platforms, one supervisory control and data acquisition (SCADA) computing platform, one GPS clock (Network Time Protocol [NTP] server) and one Unified Threat Management (UTM) Firewall. The UTM serves as the boundary protection firewall and interconnection to the SCADA Control Center and also facilitates remote access to the protection IEDs. Furthermore, independent connections exist on the IEC 61850 station bus for transmitting GOOSE messages between substations for purposes of sending carrier send/receive signals. The use of SDN supports the provisioning of independent physical communication circuits between substations. Each circuit is based on PRP with local-area network (LAN) A communicating over the ELES MPLS network and LAN B communicating over the ELES SDH Network. The SAN network consists of 28 meters, 13 PMUs, 4 power quality devices, 2 transformer monitoring devices, and 1 reactor monitoring device.

It was observed that not much interaction and data transfer was needed between voltage levels. The use of SDN supported the separation of the network between voltage levels. This provided ELES with the ability to operate the 400kV substation network uninterrupted if the 110kV system is unavailable. This separation also facilitates easier troubleshooting of the network and provides a mechanism to expand the system and manage the increase of traffic on the network for expansion and provisioning the use of Sampled Values on the system during future upgrades.

B. Communications Data Flow

To prepare the communication profile and data flow of all IEDs on the network as shown in Figure 1, required an understanding of the communication exchange that takes place between the IEDs. Provisions had to be made for the following data exchanges:

- Each device communicates with the GPS Clock (NTP server) for time synchronization
- The station and SCADA computer communicates to all IEDs in the substation for monitoring and control
- The Bay Computer communicates plant information for interlocking
- Communication for device configuration
- Remote communications for capturing disturbance records from protection IEDs
- Remote communications for remote engineering access

User manuals from equipment manufacturers were used to determine the type of traffic and data flow which exists for each device type. In cases where this information was not available, network analyzers were used to inspect the traffic from the

device. A considerable amount of information was gathered through this exercise relating to the communication profiles of each device. This information was used to define the traffic that should be authorized on the SDN network. Traffic that was learned as presented in Figure 1 included IEC 61850 MMS, NTP, GOOSE, PRP supervision packets, FTPS, SNMP Traps, and various TCP/UDP ports for device engineering software etc.

C. Traffic Prioritization

Using the data gathered on the type of traffic which exists on the network, a CoS regime was applied based on the communication guidelines defined in IEC 61850-90-4 [3]. The highest priority was assigned for transmission of GOOSE trip and distance protection messages. Thereafter, a slightly lower priority was defined for GOOSE messages used for interlocking. All MMS and other traffic were assigned a lower priority than all GOOSE messages. Subsequently, the design documents needed to be prepared for the ZTD based on the information gathered.

V. ZTD

Deploying network switches in the OT environment has become a complex task requiring engineers to perform configuration and firmware management for each individual network switch. The task of configuring network switches with the correct applications, security, redundancy and user and network management settings can be a laborious process. These tasks are further augmented depending on the size and complexity of the OT network. As the number of devices increase in the power system, device and network management can become extremely complex and network expansion can cause disruption to mission-critical networks and cause frustration to operation and maintenance engineers. Consequently, a solution is required to perform network device configuration and management across the entire device/system lifecycle and solution development process to assist in these tasks.

A. The ZTD Concept

The concept of ZTD is widely deployed in the IT and business environment [4]. It allows the provisioning of a device without the need for an engineer to manually configure each switch on the network [5]. Moreover, it reduces the time taken to deploy network switches on the system. This plug-and-play concept is not new in networking and can be used to provide different levels of automation to configure and manage the network. This provides the user with the ability to configure an entire network using a fully orchestrated platform and achieving end-to-end communications circuits or service delivery of applications on the network [6].

ZTD addresses several challenges facing utilities with configuring and managing a large number of networking devices. These include:

- Cost/Effort—the process to configure each device is costly, requires significant effort, and is prone to errors [7]. This process is simplified and cost-effective using the ZTD approach.
- Scalability—manually configuring each network switch complicates the configuration for large networks and makes network expansion a challenging task affecting the scalability of the network. This challenge is addressed using ZTD by provisioning end-to-end communications circuits without being concerned about the communications path, redundancy and configuration of each individual switch greatly simplifies the network configuration and enhances scalability of the network.
- Interoperability—Each switch manufacturer has its own method of configuring the network appliance. Supporting open-standards and Application Programming Interfaces (APIs) for network configuration and management provides great flexibility to use ZTD to fully automate the network configuration.

Based on the aforementioned, it was decided to use ZTD together with the SDN controller to fully automate the network configuration of OT SDN switches in the ELES network. This led to the development of an automated network configuration, management, and diagnostics tool to be used to configure the SDN network switches and communicate with the SDN controller (using an open-standard REST API) to provision complete end-to-end communications circuits between IEDs [8].

B. Requirements

Specific requirements may vary for different ZTD programs. The most common specific requirements include:

- The need for a communications infrastructure to support the deployment program. In this case, it was through the ELES IP/MPLS network.
- A fully automated ZTD tool that can configure each network switch automatically across the network.

During the design phase of the ZTD tool, two categories of specifications needed to be considered to address ELES's networking requirements. These included the specification for the tool itself and what level of networking automation was required. The second included the prerequisite data and format of the data needed by the tool to prepare for ZTD and successfully configure and manage the network. These two categories are described in detail below.

1) Specification of ZTD Tool

The ZTD tool must be able to provide visibility into many aspects of the system. The tool must be able to visualize the desired system design so it can be reviewed before deployment by different subject matter experts. This may take different forms depending on the task, like detailed host lists and connection details for use by the installers to ensure that the right data are being collected. Some of the specifications for the ZTD tool included:

- A method to specify IP addresses, physical locations, and connections of IEDs and switches.
- Easy to specify communication configuration between IEDs by using aliases for protocols and hosts.
- Multiple substations/networks/configurations should be represented in the same configuration documents. The ZTD tool should intelligently manage the separation of data to ensure that only the desired circuits and substations are configured.
- A process should run to make a complete ground up reproduction of the whole network from a single set of configuration documents. This will also facilitate the production of repeatable and predictable behavior.
- A mechanism should exist in the tool to verify the design against the configuration and verify the configuration against what has been deployed on the network. Consequently, reports should be available to ELES to show the difference between the live network and the desired configuration.
- When updating the network with changes, the ZTD tool should only update the differences across the network. Existing communication circuits should not be modified. It must be possible to do a health check / difference report on the network at any time to make sure that the active configuration matches the desired design. A report showing any differences must be created if any exist. This difference report would be used during maintenance or modifications to the network to make sure that desired changes are what is expected before the changes are applied to the live system.
- When automatically deploying the network configuration any errors found during deployment must be reported to the user.

The ZTD tool should also provide a series of reports which can be used by ELES during the lifecycle of the network at ELES. Reports detailing every communication circuit provisioned in the system must be available during the factory acceptance test (FAT) and site acceptance test (SAT) to allow a complete checkout of all allowed communications on the system. This report, because it details every conversation that is allowed on the network and includes the details of the devices involved, would be used when troubleshooting any communication problem. This same report can be used for periodic baselining and audit reports to check the status of the system. Because of the deny-by-default nature of the SDN system, troubleshooting is greatly enhanced by looking at the flow counters and the packets that are denied by the current network configuration, both of which are available from the SDN controller.

2) Preparation for Zero Touch

The whole configuration for every aspect of the network must be contained in the configuration documents. These documents can then be consumed by the ZTD tool as a prerequisite to connect to the SDN controller and automate the network configuration. Prerequisites for the ZTD tool include:

- Compiling a list of applications and protocols used on the network.
- Understanding the topology of the network.
- Documenting the redundancy requirements considering Dual Attached Nodes and SANs.
- Planning the communications path.
- Performing a site audit and/or capturing and analyzing traffic from a traditional Ethernet network to understand the data flow and communications profiles.
- Understanding the latency and jitter requirements.
- Analyzing bandwidth and wide-area network (WAN) infrastructure constraints (if applicable). This includes the location of the SDN controller and ZTD tool and connectivity to all the network switches for configuration and management.

A Microsoft Excel template was used to document the aforementioned networking information for each substation in order for the ZTD tool to directly consume and automate the network configuration. Figure 2 illustrates the workflow used by ZTD tool.

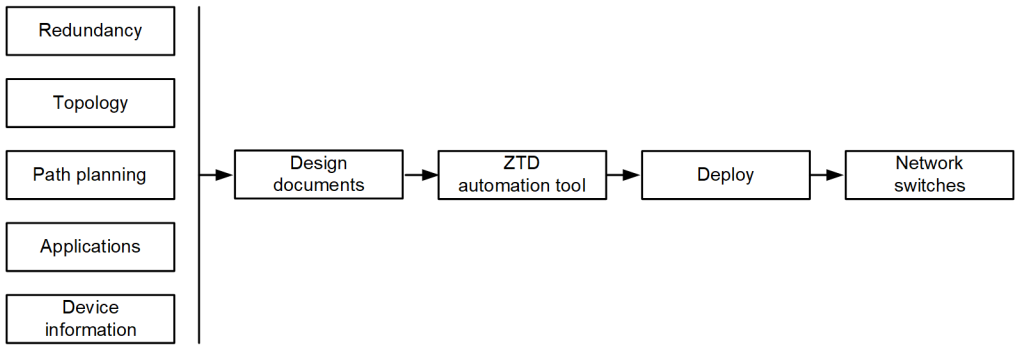

Figure 2 Workflow of the ZTD tool developed for SDN deployment.

C. Functional Description

This ZTD tool can be described in three general functions: 1) Design 2) Configuration 3) Diagnostics, as illustrated in Figure 3. These do not form a one-way process, but each function is affected by the other and affects other functions. For example, if after the configuration was applied a circuit was missing, then the design would be updated and the updated configuration would be applied.

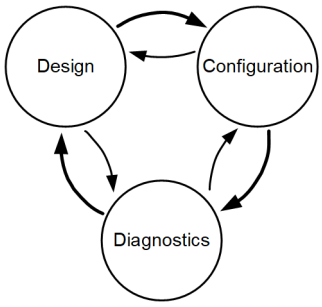

Figure 3 Workflow representing the primary ZTD functions.

1) Design

The purpose of the design is to have a system-independent method of compiling and sharing information with all stakeholders at ELES. The documentation does not need to be complex but should be human readable. A simplified description of the documentation for this system follows.

The design of this system included two general parts: description of the IEDs and the circuits. The IED design part involved documenting the devices by documenting settings such as name, IP address for hosts and specific switch settings, such as IP address and controller IP address used for the switch configuration. The circuits part of the design consists of three parts: IEDs documented previously, the communications profiles, and the specific communication circuits. The communication profiles provide a template that can be referenced in defining the specific communication circuits.

As depicted in Table 1, a profile is created for a GOOSE machine-to-machine (M2M) application that defines configuration information used by the switch when generating the circuit: specifically what MAC address and VID was assigned to the protocol.

TABLE 1
BRIEF EXAMPLE OF A PROFILE DEFINITION

Name	Ethernet destination	VLAN ID (VID)
GOOSE M2M	01:0C:CD:00:00:01	123

As shown in Table 2, a user-defined two IEDs, along with the profile used to communicate with the destination(s). Some derivable traffic, such as ARP, the most common, does not need to be specified unless there is a special case. If a device communicates a unicast IP protocol such as MMS within the LAN, then ARP must be present, so the communications circuit can be generated automatically by the ZTD tool and does not need to be documented explicitly.

TABLE 2
BRIEF EXAMPLE OF A DEVICE AND CIRCUIT DESIGN

Device	Communication profile	Destination
Teleprotection device	NTP Client	NTP Server
	GOOSE M2M	Protection Relay 1
Protection relay	NTP Client	NTP Server

Most host IEDs consist of protection relays, bay controllers, SCADA servers and GPS Clocks. However, other devices are also present including network switches and MPLS routers. The ZTD tool introduced an algorithm for intelligent packet coloring using VLAN IDs (VIDs), with the goal to facilitate and automate the creation of SDN rules (or flows) needed for communications across the MPLS WAN network. The MPLS network required packet coloring, so the design also included which VID was needed and the configuration applied the coloring.

Also included in the design is assigning each device port to a network designation, i.e., the network it belongs to and the substation. In the case of the network, it could be a SAN or one of the PRP networks (LAN A or LAN B) with one interface belonging to each. Hence, a PRP device in Substation X would have two ports, one belonging to Network X and LAN A and the other to X and LAN B. A SAN port would be connected to X and SAN. These networks allow smart division of devices that can form a minimum collection to apply a configuration to.

2) Configuration

Synchronizing the design to the system involves two general steps: 1) initial configuration of the SDN network switches and adding the settings for the IEDs to the SDN controller so the paths through the substations are identified, and 2) applying the end-to-end communications circuits to the network switches so device communications is possible over the identified paths. This configuration is applied by the ZTD tool by intelligently checking for differences in the configuration and applying the necessary changes.

The important benefit of automation is that the design documents were used in the generation of the entire configuration directly and manual configurations processes were eliminated as depicted in Figure 4. This simplifies the change control mechanism as changes in the design can be applied directly using a predicable automation pattern.

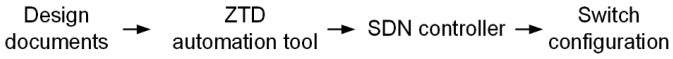

Figure 4 Network configuration workflow.

If both the source device and destinations device(s) are connected to the network using PRP, the LAN A and LAN B networks are both assigned the same communication circuits to keep both LANs synchronized and ARP circuits are added where needed without extra design complexity.

As some substations may be in operation while some are undergoing refurbishment or construction, the changes are applied on a per substation, per-LAN basis, so the differences are applied in a controlled manner. This presented a significant benefit to ELES as the configurations for refurbishment

projects and new substations could be processed using the ZTD tool while keeping the existing network completely operational and unaffected.

3) Diagnostics

The diagnostic function of the ZTD tool is used to diagnose, find root cause, or find a remedy to issues in the configuration or execution of the automation. This function can be divided into three categories: design, configuration, operational.

Checking the design includes checking that the same hostname is not entered twice and that values are placed where they need to be or, importantly, where they should not be and that a referenced communication profile and destinations exists.

Configuration diagnostics is used to check the configuration, such that IP addresses are unique or that a communication circuit is in the success state and other various checks that cannot be performed in the design function.

Operational issues include why a communication circuit is in success, but traffic is not flowing, which might occur if the IP address is incorrect or the communication circuit itself does not properly match the communication traffic being exchanged or some other traffic needs to be enabled for the circuit to work.

The SDN network switches and the SDN controllers generate data in various forms which can be mutated into different forms to provide additional ways to troubleshoot issues. The network switches themselves provide diagnostics such as counters for each hop of a circuit which can be collected and displayed to determine if traffic is flowing along the programmed path.

SDN network switches have the ability to forward denied traffic or traffic that does not match any specific rules to an intrusion detection system (IDS) sensor or network analyzer. This unmatched traffic can potentially arise due to misconfiguration or due to malicious intent. An important part of a functioning diagnostic system is to collect the unmatched traffic and create the necessary configuration to forward it to a sensor, network analyzer or IDS to identify traffic that IEDs are sending that do not match any of the current communication circuits: either unintentional or intentional (malicious or configuration-related). The controls for this are also part of the design.

The troubleshooting function may also be proactive. The ZTD tool includes a process to detect some potential operational problems. Increased troubleshooting tools have been developed over the life of the project and during the maintenance phases of the project including simulation of traffic to confirm path planning of the circuit is correct along with co-location of flow counters with path information to detect problems with traffic forwarding.

D. Design Considerations

There were several design considerations which needed to be taken into account due to their effect on the functional process of the system. The system includes both active networks (LAN A and LAN B), networks in FAT/SAT, or in construction. For this reason, the configuration is applied on a per-LAN basis, so the other networks are not affected. The substations are often not attached to each other so one controller controls multiple disjointed substations and the switch management traffic is managed through the MPLS network outside of the LAN. Within the LAN the switch management traffic (or in-band management traffic) is handled as if the controller was directly connected.

Traffic may have three different domains based on where it originates and terminates: within a substation, between a substation and device beyond the MPLS network, and traffic that is exchanged between two substations. The first two are managed in the tool by selecting the appropriate substations and LAN network designations and the latter is managed by selecting two substation network designations, which instructs the ZTD tool to manage only the intrasubstation traffic. The MPLS network uses the coloring algorithm to correctly forward traffic across the WAN. The design function, therefore, as stated also included coloring information (using VIDs) that is applied to the Ethernet packets egressing to and ingressing from the MPLS network.

There are two network controllers, one for LAN A and the SAN network and one for LAN B. There is a single set of design documents used by the ZTD tool to apply the appropriate configuration based on the controller it is configuring.

In large networks and/or networks with a lot of communication circuits, switch resources may be at a premium so adding additional cables can decrease the number of path hops which decrease total resources for a circuit. This does require adjustment to the circuit provisioning algorithm to produce the required path. Algorithms were developed to look at the effect of this.

E. Benefits

The concept of zero touch helps network engineers begin a progressive and steady transition from a vulnerable RSTP-based managed switch network to a secure software-defined network. In addition to the security and network management benefits, using the ZTD tool together with SDN provided several additional benefits to ELES which included:

- The streamlined process saved time, cost, and labor.
- Reduced the risk of human error and provided automated error-checking capabilities [4].
- Automated process increased productivity [7].
- The ZTD tool connects to the trusted SDN controller.
- Through the process of adoption, SDN network switches can be configured to only communicate with its intended SDN controller and prevent users from connecting another SDN controller to the network for any malicious intent of changing or manipulating settings [4].
- Network automation replaces manual tasks for a predictable and repeatable approach [7].
- Ability to configure multiple substations from a system-independent set of network documentation.

In some cases, it also reduces travel costs, labor overhead and allows commissioning engineers to focus on other operational tasks like preventative and reactive maintenance work.

VI. Challenges

Security requires knowledge of the underlying system to learn and understand what traffic should be allowed and what should not. Traditionally, little attention has been paid to protocol details for communications required to setup different system functions because a traditional Ethernet network provides an open, allow-all, security model for communications within substations and TCP/UDP filter is only applied at the edge or the electrical security perimeter of the substation. Consequently, often information is incomplete on what network traffic and data flow needs to be present for each function on the IED, especially for devices communicating within the substation. A significant challenge, therefore, has been obtaining this information, either from manufacturer documentation or through diagnosing. For example, some traffic may require PRP supervision traffic to function and some does not, but this information is not included with device instruction manuals. This challenge is further exacerbated when considering legacy devices. However, this process only needs to be performed once and can then be used for future projects.

Another challenge which needs to be considered is that the introduction of new technology requires thought on how to apply it to current processes and how to adapt new processes to the new technology.

VII. Looking Ahead

Over time, both the ZTD tool and the underlying controller have improved. Several future changes to the controller will enhance the ZTD automation capabilities. These include:

- Lock settings so that the system/switches do not accept unintentional changes for increased reliability.
- Increased support for meshed networks in path planning and path display.
- A two-dimensional topology display, along with other scalability improvements to manage the increasing number of disjoined LANs.
- Apply a zero-touch firmware deployment function on network switches.

Several future design improvements include:

- Mirroring traffic to send a copy to a traffic analyzer.
- Increased use of telemetry and visualization techniques to view diagnostics or other time dependent data over time to detect trends and problems.
- Enhance the configuration management function to include revision tracking from source design documents to the final deployed configuration.

VIII. Conclusion

Securing communications across critical infrastructure networks is becoming more and more essential as utilities exploit the benefits of IEC 61850 technologies in modern substation automation systems. This paper explored the benefits of implementing SDN to address the security risks presented in RSTP-based managed switches. In addition to the security concerns affecting these networks, the configuration and management of networking switches is a complex task, and this complexity increases as the number of devices and types of communications in the network, such as IEC 61850, continue to grow. ZTD is a process whereby the required device communications is automatically provisioned without the need of any direct manual intervention on the device. To achieve these benefits, this paper described an innovative solution using ZTD together with SDN through a real-world project implemented by the ELES TSO in Slovenia. During the project, an intelligent ZTD tool was used to deploy this solution in a transmission substation. The user requirements, specification and design of the tool, associated benefits of this solution, and the hurdles resolved during the project were also covered.

IX. References

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

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

[3] IEC TR 61850-90-4, Communication Networks and Systems for Power Utility Automation – Part 90-4: Network Engineering Guidelines, 2020.

[4] National Cyber Security Center, "Zero Touch Enrolment," June 2021. Available: https://www.ncsc.gov.uk/collection/device-security-guidance/getting-ready/zero-touch-enrolment

[5] Microsoft Corporation, "Zero touch deployment: a cornerstone of modern device management," 2019. Available: https://www.microsoft.com/cms/api/am/binary/RE4yfB2

[6] Demchenko Y, Filiposka S, and de Vos M, "ZeroTouch Provisioning (ZTP) Model and Infrastructure Components for Multi-Provider Cloud Services Provisioning," November 2016.

[7] Anand V, "How Zero Touch Will Transform IoT Device Deployment," Capgemini Engineering, 2021. Available: https://prod.ucwe.capgemini.com/wp-content/uploads/2023/03/How-Zero-Touch-Will-Transform-IoT-Device-Deployement_Whitepaper_November-2021.pdf

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

X. Biographies

Darko Bordon joined the ELES Transmission System Operator in Slovenia in 1999 and currently holds the position of project manager and secondary systems engineer. Darko is responsible for secondary systems projects, station communications concepts, station bus commissioning, factory acceptance tests, and site acceptance tests. In 2001, he received his BSc from the University of Ljubljana, Slovenia, graduating at Faculty of electrical engineering.

Robert Meine is a graduate of the University of Idaho, where he received a BS degree in materials science and engineering and a BS degree in computer science. Robert joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2013 and is currently an application engineer in the communications department of research and development, where he supports SDN-related products.

Sagar Dayabhai is a senior application engineer for Schweitzer Engineering Laboratories, Inc. (SEL) in Europe. Sagar received his BSc Electrical Engineering degree from Wits University, South Africa and earned his MSc Electrical Engineering from Wits in 2014. He is a registered professional engineer with the Engineering Council of South Africa (ECSA). Sagar was one of the IEC Young Professionals elected for South Africa in 2016 and is currently a member of IEC TC 57 WG 10 and WG 15. After working at Eskom in the field of telecommunications and SCADA, he later moved to Consolidated Power Projects (CONCO) and held positions as a senior SCADA/automation engineer and the system control manager. Sagar has been extensively involved in cybersecurity, renewable energy systems, SCADA control systems, DMS,

substation automation, and integration of embedded generators into utility networks for more than 10 years.

Jason Dearien has been at Schweitzer Engineering Laboratories, Inc. (SEL) for over 20 years and is currently a principal application engineer in the SDN R&D Department specializing in OT SDN. He is involved in support and training for OT SDN network deployments and solutions for both internal and external customers. Previously, Jason worked in many R&D groups as a senior software engineer, leading system and architectural deployments, including the first IEC 61850 offering. He was the technical and team lead on product developments, including real-time automation controller (RTAC) and switch products.

20230526 • TP7122-01