SIMPLIFYING NERC CIP COMPLIANCE WITH SEL SDN

Lance Dice
Schweitzer Engineering Laboratories, Inc.

Kurt Kaltmaier
Guidehouse

Introduction

As power system control networks become more complex, understanding what's happening on the networks can be challenging and networks can be hard to secure. To address this concern and protect power system infrastructure, NERC CIP-007-6 R1.1 requires utilities to document which ports and services are open on each applicable bulk electric system (BES) cyber asset, including IEDs, where technically feasible [1]. Knowledge of ports and services is also beneficial for NERC CIP-010-2 R1.1.4, which requires utilities to develop and maintain baseline configurations to ensure secure change management on all logical network-accessible ports on applicable BES cyber assets [2].

This paper describes how SEL software-defined networking (SDN) can significantly reduce the time and effort required to collect data and provide evidence for CIP-007-6 R1.1 and CIP-010-2 R1.1.4 compliance. It also describes how SEL SDN can assist with meeting NERC CIP-005-5 R1.1—3 requirements [3].

CIP-007-6 R1.1—Documenting Open Ports and Services

CIP-007-6 addresses system security management. It requires utilities to define methods, processes, and procedures for securing cyber assets within the electronic security perimeter and includes technical, operational, and procedural requirements. Subsection R1.1 addresses ports and services, stating: "Where technically feasible, enable only logical network-accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device, then those ports that are open are deemed needed" [1].

To comply with R1.1, utilities must collect data when using legacy Rapid Spanning Tree Protocol (RSTP)-based networking. Thorough data collection is not possible at the switch level and must be collected at the IEDs for the following reasons:

- All communication is controlled at the IED level because there is no TCP or UDP filtering done on the switches.
- IEDs can communicate however and with whichever device they want on the same VLAN.

Accurate data collection requires querying all devices on the network for open ports and services. Running port scans in a live operational technology (OT) environment is time-consuming, redirects critical labor resources, and is costly and challenging because it impacts live communications by placing unnecessary traffic on the network. The extra traffic injected on the network during automated port scans can be dangerous in a substation environment, causing performance or availability issues. Due to this invasive and potentially disruptive operation, automated scans are usually only recommended in a controlled environment. Thus, device interrogations are typically done manually by reading the device configuration for IEDs, which is potentially less accurate than using a port scan.

CIP-010-2 R1.1.4—Developing a Baseline Configuration for Open Ports

CIP-010-2 addresses configuration change management. It requires utilities to develop and maintain baseline configurations for applicable cyber assets, and Subsection R1.1.4 is specific to any logical network accessible ports. As with CIP-007-6 R1.1, the registered entity must be aware of open network ports and services [2]. Routine scanning is a common method to determine open ports and services. Often, software or patches and updates can expose additional ports or services without the administrator's awareness. Undefined or undocumented ports and services may pose a security risk for the utility and can be a potential compliance concern for both CIP-007-6 R1.1 and CIP-010-2 R1.1.4. Only expected open ports and services should communicate on mission-critical OT networks.

NERC CIP Compliance Made Easier by SEL SDN

SEL SDN helps utilities improve cybersecurity and automate data collection for NERC CIP reporting. An SEL SDN network is made up of two parts, as shown in Figure 1. The first part is the SEL-2740S Software-Defined Network Switch, the physical switching hardware. The second part is the SEL-5056 Software-Defined Network Flow Controller, and the controller software allows users to

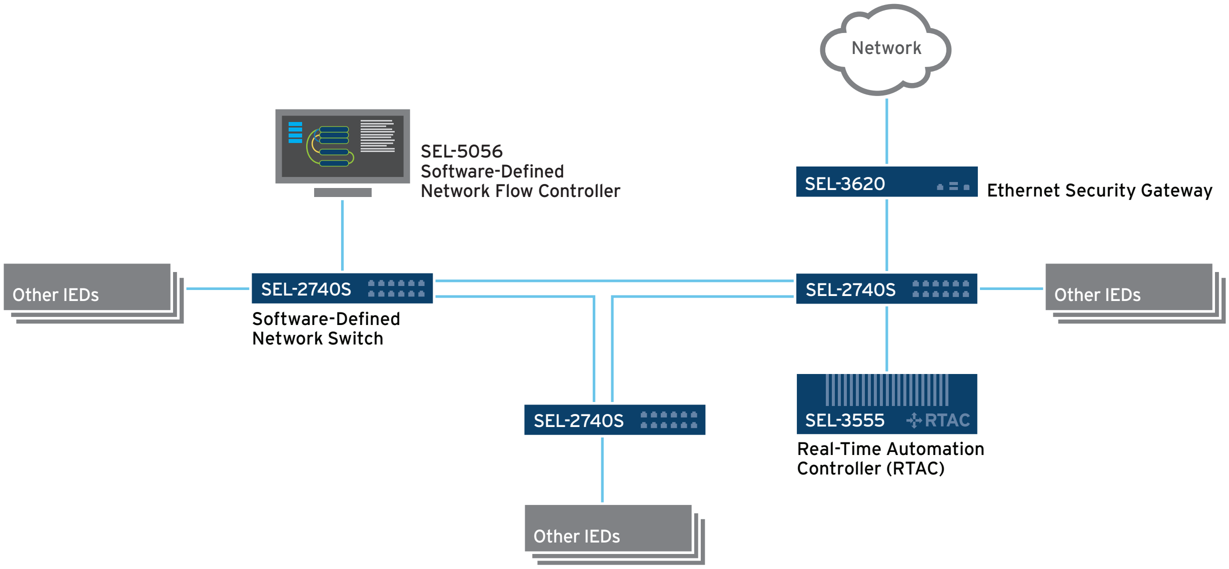


Figure 1—SEL SDN substation network.

configure the SEL-2740S switches. All communications flows in the network are programmed into the SEL-2740S switches using a deny-by-default approach. Users can filter traffic using packet attributes in transport Layers 1 through 4 inline at the switch and can limit available logical ports for connected devices, resulting in a more secure network that is purpose-engineered for required applications.

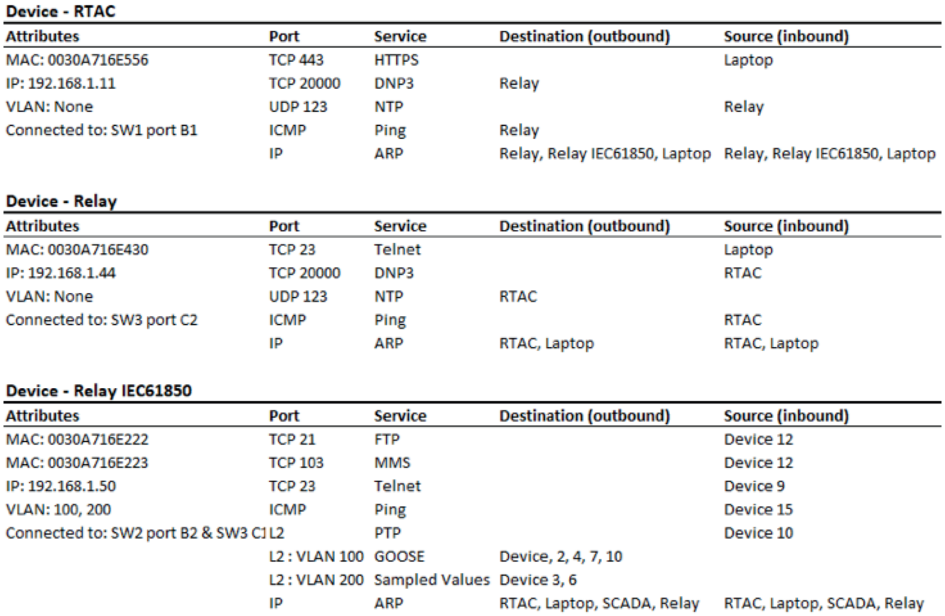
Predetermining network flows with SDN not only makes the data paths clear, but also improves security. The CIP-007-6 Guidelines and Technical Basis states, "This control is another layer in the defense against network-based attacks, therefore the SDT [Standard Drafting Team] intends that the control be on the device itself or positioned inline in a non-bypassable manner" [2].

By configuring the network in a way that all devices are only connected directly to the SEL-2740S switches, there are records as to what type of traffic a device can send and receive as well as the source and destination device(s) of that traffic. This allows the utility to determine exactly which ports and services are allowed for communication to each device and ensures that once the network is engineered, no new network traffic is allowed until the utility makes a configuration change.

This switch architecture, with all network conversations configured in the flow controller, simplifies compliance with CIP 007-6 R1.1 and CIP-010-2 R1.1.4. The flow controller maintains a database of the type of traffic a device can send or receive as well as the source and destination device(s) of the communication, aiding compliance with the NERC CIP record-keeping requirement.

SEL Flow Auditor—A Powerful Reporting Tool

Flow Auditor is an application in the SEL-5057 SDN Application Suite that can interface with an SEL-5056 controller to generate reports based on network flows in an SDN network. These reports, like the example in Figure 2, list the individual hosts and known attributes, including the IP address, MAC address, VLAN(s), location of physical connection, and ports and services communicated to and from the host. This allows the rapid, on-demand gathering of information



Device - RTAC

Attributes	Port	Service	Destination (outbound)	Source (inbound)
MAC: 0030A716E556	TCP 443	HTTPS		Laptop
IP: 192.168.1.11	TCP 20000	DNP3	Relay	
VLAN: None	UDP 123	NTP		Relay
Connected to: SW1 port B1	ICMP	Ping	Relay	
	IP	ARP	Relay, Relay IEC61850, Laptop	Relay, Relay IEC61850, Laptop

Device - Relay

Attributes	Port	Service	Destination (outbound)	Source (inbound)
MAC: 0030A716E430	TCP 23	Telnet		Laptop
IP: 192.168.1.44	TCP 20000	DNP3		RTAC
VLAN: None	UDP 123	NTP	RTAC	
Connected to: SW3 port C2	ICMP	Ping		RTAC
	IP	ARP	RTAC, Laptop	RTAC, Laptop

Device - Relay IEC61850

Attributes	Port	Service	Destination (outbound)	Source (inbound)
MAC: 0030A716E222	TCP 21	FTP		Device 12
MAC: 0030A716E223	TCP 103	MMS		Device 12
IP: 192.168.1.50	TCP 23	Telnet		Device 9
VLAN: 100, 200	ICMP	Ping		Device 15
Connected to: SW2 port B2 & SW3 C1	L2	PTP		Device 10
	L2 : VLAN 100	GOOSE	Device, 2, 4, 7, 10	
	L2 : VLAN 200	Sampled Values	Device 3, 6	
	IP	ARP	RTAC, Laptop, SCADA, Relay	RTAC, Laptop, SCADA, Relay

Figure 2—Flow Auditor report example.

for CIP-007-6 R1.1 and CIP-010-2 R1.1.4 baseline evidence without invasive port scans. It takes mere minutes to obtain accurate evidence for compliance reporting and eliminates the need for manual auditing.

Flow Auditor also makes it possible to compare older and newer reports to see and verify changes in the network. Archiving the reports gives a historical view of the network. Comparison allows the reports to be used for change control of a network.

In addition to providing data for compliance reporting, Flow Auditor also assists with managing installed device inventory, performing security audits, and validating network/dataflow diagrams. With Flow Auditor, utilities can know exactly which devices are on the network and where the devices are located.

Additional Benefits of SDN for NERC CIP Compliance

In addition to providing information that can benefit CIP-007-6 R1.1 and CIP-010-2 R1.1.4 compliance, SEL SDN can also assist with CIP-005-5 R1.1—3.

CIP-005-5 R1.1 requires that the cyber assets connected to a network with a routable protocol are contained in an electronic security perimeter (ESP) [3]. The SEL-5056 controller’s topology management view displays all devices present on the network and which SEL-2740S the applicable BES cyber assets (BCAs) are connected to, as shown in Figure 3. This gives a complete view of the current network and identifies all connected devices while defining the ESP boundary and providing an electronic access point (EAP).

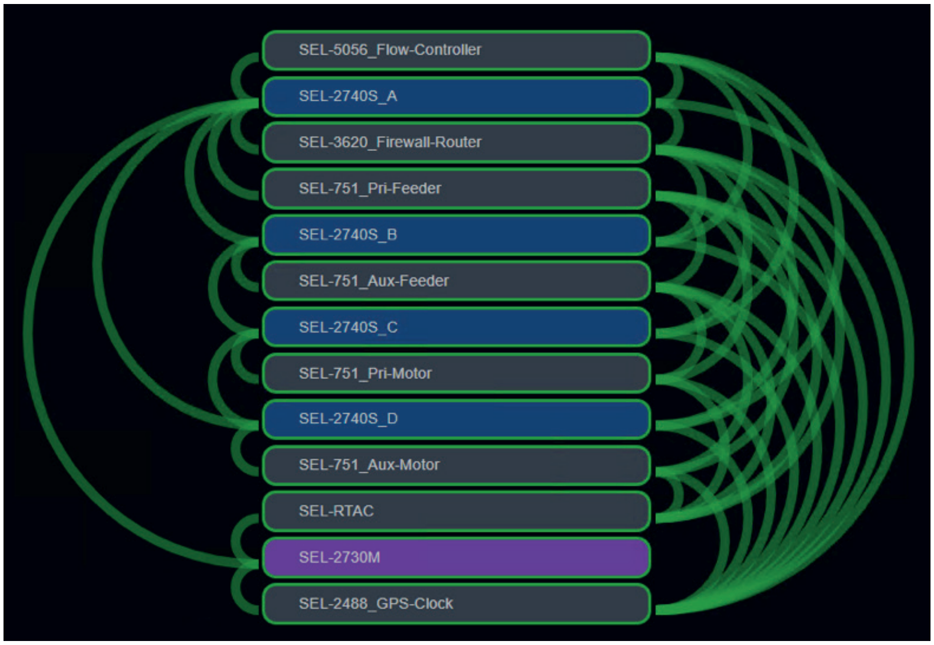
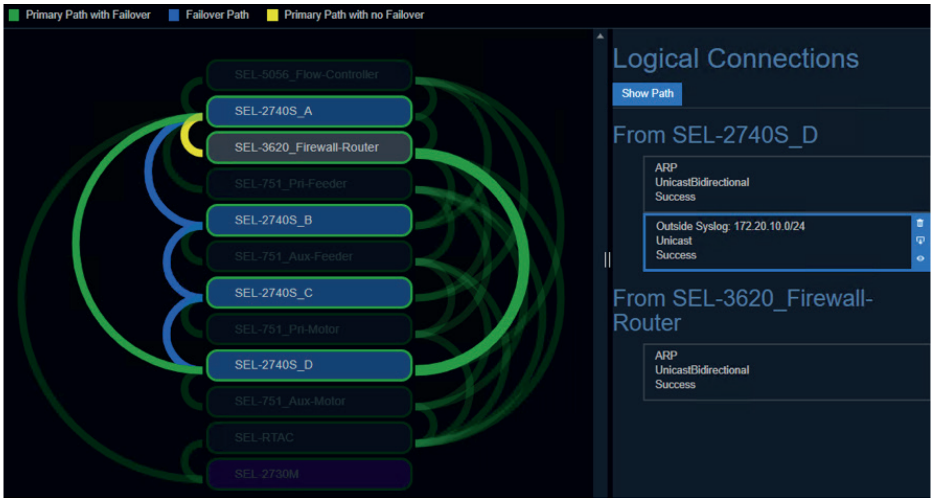


Figure 3—A fully adopted network with logical connections.

CIP-005-5 R1.2 also requires that all external routable connectivity go through a defined EAP [3]. When using logical connections, the SEL-5056 topology view can display the exact path (including a backup path) that traffic will travel, as shown in Figure 4. This allows a utility to verify the traffic only flows where it is explicitly allowed and provides the ability to verify the traffic flow against a dataflow diagram. Utilities may define multiple EAPs for an ESP, as required for backup flow paths.



Logical Connections

From SEL-2740S_D

ARP
UnicastBidirectional
Success

Outside Syslog: 172.20.10.0/24
Unicast
Success

From SEL-3620_Firewall-Router

ARP
UnicastBidirectional
Success

Figure 4—Logical connection allowing "SEL-2740S_D" to send Syslog messages to an outside network through the SEL-3620.

CIP-005-5 R1.3 states that utility networks must "require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default" [3]. When configuring an SEL SDN network, the user whitelists traffic, which leaves all other traffic denied by default. The user can also name logical connections and include the traffic type.

Conclusion

An SDN network with Flow Auditor eliminates the need to run port scans on power system control networks. It's a noninvasive, safe, and fast way to collect the necessary network flow information for NERC CIP compliance. Additionally, it removes the need for a user to manually audit individual hosts of the network, saving time on a tedious task. Instead of requiring hours to scan and audit a substation for CIP-007-6 and CIP-010-2 R1.1.6 compliance, the Flow Auditor provides accurate evidence in minutes. It also provides some of the data required to comply with CIP-005-5.

Flow Auditor can also assist with managing installed device inventory by showing exactly what devices are on the network and where they are located. This is a powerful tool not only for NERC CIP compliance but also for security audits and network and dataflow diagram validation.

SEL SDN allows the user to have total control and visibility of their network as a whole, enabling the development of a more secure network that is purpose-engineered for required applications. The increased awareness provided by SDN gives a better view of which devices are connected to the network and how they communicate.

References

[1] NERC Standard CIP-010-2 — Cyber Security Configuration Change Management and Vulnerability Assessments. Available: nerc.com.

[2] NERC Standard CIP-007-6 — Cyber Security Systems Security Management. Available: nerc.com.

[3] NERC Standard PRC-005-5 — Cyber Security Electronic Security Perimeter(s). Available: nerc.com.

Biographies

Lance Dice, CISSP, has a BAS in information systems analysis from Lewis-Clark State College. He works at Schweitzer Engineering Laboratories, Inc. (SEL) as an application engineer in Research and Development. He has been at SEL for over 7 years and has been involved with Information Security, Engineering Services, and now Research and Development as part of the software-defined networking team. Lance is a Certified Information Systems Security Professional (CISSP).

Kurt Kaltmaier, PMP, CISSP, has a BS in business management from Redlands University. He is a managing consultant at Guidehouse (Guidehouse.com) which specializes in energy and utility cyber security and NERC CIP compliance. Kurt has been with Guidehouse (formerly Navigant) for one year; prior to that, he led a consulting team at Schweitzer Engineering Laboratories, Inc. (SEL), focusing on cyber security and utility compliance for nearly four years. Prior to working at SEL, Kurt managed IT and compliance teams at San Diego Gas and Electric for 15 years. He is both a Project Management Professional (PMP) and a Certified Information Systems Security Professional (CISSP).

SEL SCHWEITZER ENGINEERING LABORATORIES

Making Electric Power Safer, More Reliable, and More Economical
+1.509.332.1890 | info@selinc.com | selinc.com

LWP0033-01 • 20200330

LWP0033-01