SOFTWARE DEFINED NETWORKING

Transforming Network Reliability at New Indy Containerboard With SDN

Tyler Songstad, Charles Carroll, Andy Gould, and Will Edwards
Schweitzer Engineering Laboratories, Inc.

Introduction

New Indy Containerboard, located in Catawba, South Carolina, faced significant challenges with their Ethernet network. This network, crucial for their industrial control systems, frequently failed, causing production halts and significant downtime. To address these issues, New Indy partnered with SEL Cyber Services to implement a software-defined networking (SDN) solution tailored for operational technology (OT) networks.

The Challenge

New Indy's power system control network consisted of various protective relays, meters, drives, and programmable logic controllers, all interconnected through a mix of managed and unmanaged Ethernet switches in a mix of radial and partial-ring topologies. This architecture utilized one managed switch per network and used the Rapid Spanning Tree Protocol (RSTP) to prevent network loops. While the redundant connection to the head switch was intended to provide some minimal redundancy, this simplistic network design combined with the use of RSTP resulted in a network that lacked resiliency, determinism, and security.

Traditional Ethernet networks operate on the principle of best-effort delivery of packets, relying on network infrastructure design, subnetting, and VLANs to shape, forward, and deliver Ethernet traffic. Newly introduced Ethernet hosts send Address Resolution Protocol (ARP) messages, broadcasting their presence to the network, including the physical MAC address as well as the IP address assigned to the device, which are registered to switch ARP tables. Traditional Ethernet switches use protocols to determine neighboring switches, establish the root bridge, and recover from link failures. This is by design and has been engineered for convenience, as most IT networks are dynamic and need to operate on a plug-and-work principle whereby a new host can be either statically or dynamically assigned an IP and join a network. Hosts on IT networks leveraging managed switches can rely on error checking within protocols and retries to overcome transient outages or changes in the network topology. For instance, if a user hits "Send" on an email and it takes an additional 500 ms or more to send it out to the network during a network reconfiguration, most users are wholly unaware of that delay.

This reconfiguration or reconvergence is typically achieved using RSTP, which is deployed to prevent network loops and determine alternate network paths in the event of a link failure. RSTP works automatically when enabled but requires time for all the switches in the topology to participate in the healing algorithm. This reconvergence time can result in packet loss, which must be overcome by resending or retrying the delivery of traffic on IT networks. As networks get larger, this reconvergence time increases with the number of nodes participating in the network. Due to the dynamic nature of RSTP, reconfiguration times can vary, making it infeasible to accurately predict and model failure modes or fault conditions. Combining RSTP with unmanaged switches or using default configurations on managed switches further accentuates this ambiguity.

Standard Ethernet in IT networks does not allow for redundant network paths, but newer protocols and architectures, such as the Parallel Redundancy Protocol (PRP) and High-Availability Seamless Redundancy (HSR), have been added to Ethernet networks as a means of addressing the issue of packet loss. However, these architectures typically require a significant expansion in scope and cost of network design or require specialized hardware for duplication and deduplication of messages.

Redundancy and mitigation of packet loss are particularly important in OT networks, like industrial process control, manufacturing, and utility systems, because missing a critical stop, start, trip, close, or other control intervention message could be catastrophic. These OT networks also have far less need for the dynamism required to provision IT network traffic in such places as offices, coffee shops, or schools. The hosts that participate in OT networks are typically well documented and static, and they require deterministic response and healing intervals for closed-loop feedback.

The manufacturing process control system at the New Indy plant relies upon feedback from the power delivery system across the plant, via Modbus TCP, to a pair of dual-redundant controllers in each system: one pair for the stock prep process and one pair for the dry end process. These networks have always been independent, and management desired to maintain the independent design of these plant processes, as each is supported by different departments. The loss of Modbus telemetry from the power system network, which occurred each time the Ethernet switch system failed to recover from a problem, eventually forced the manufacturing process on either the stock prep or dry end network to come to a halt. This disruption caused not only lost time and production, but a significant amount of work to clear the in-process material before they could restart production.

For New Indy, this setup lacked redundancy and visibility, making troubleshooting nearly impossible. Frequent network outages disrupted the manufacturing process, leading to costly production stops and extensive recovery efforts. As these outages became more frequent—and easy answers to determine the source of the problems nearly impossible to find—management was highly motivated to affect change at the plant.

The Solution

SDN engineered for OT reimagines the process for designing reliability and redundancy within critical infrastructure by removing the distributed decision making inherent to IT networks and moving the control plane to a software-based top-level network controller, which can control the behavior of the network traffic between hosts, referred to as traffic flows, to the performance requirements of the system. By centralizing this flow controller above the network of switches and hosts, network administrators can prescribe exactly what traffic is allowed between each host and how to proactively ensure secondary network paths are available to fail over to within microseconds of the loss of a network asset, be it a port or cable or switch.

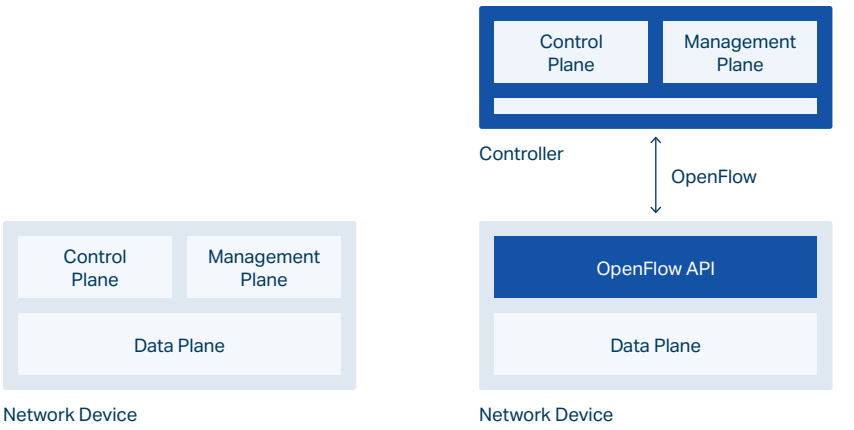

Figure 1—Traditional network compared to SDN

SEL Cyber Services proposed an engineered SDN-based solution to replace the fragile New Indy networks. The new architecture included SEL-2740S Software-Defined Network Switches configured to provide path redundancy, security, and enhanced network visibility.

To support the goal of these new networks, SEL created a new network topology that incorporates primary and backup network paths for the SEL-2740S SDN switches. Switch locations included a combination of medium- and low-voltage switchgear or motor control centers. To align with the New Indy philosophy of keeping networks independent, a dedicated SDN flow processor computer was provided for both stock prep and dry end networks to configure and monitor the system.

SDN Network Topology

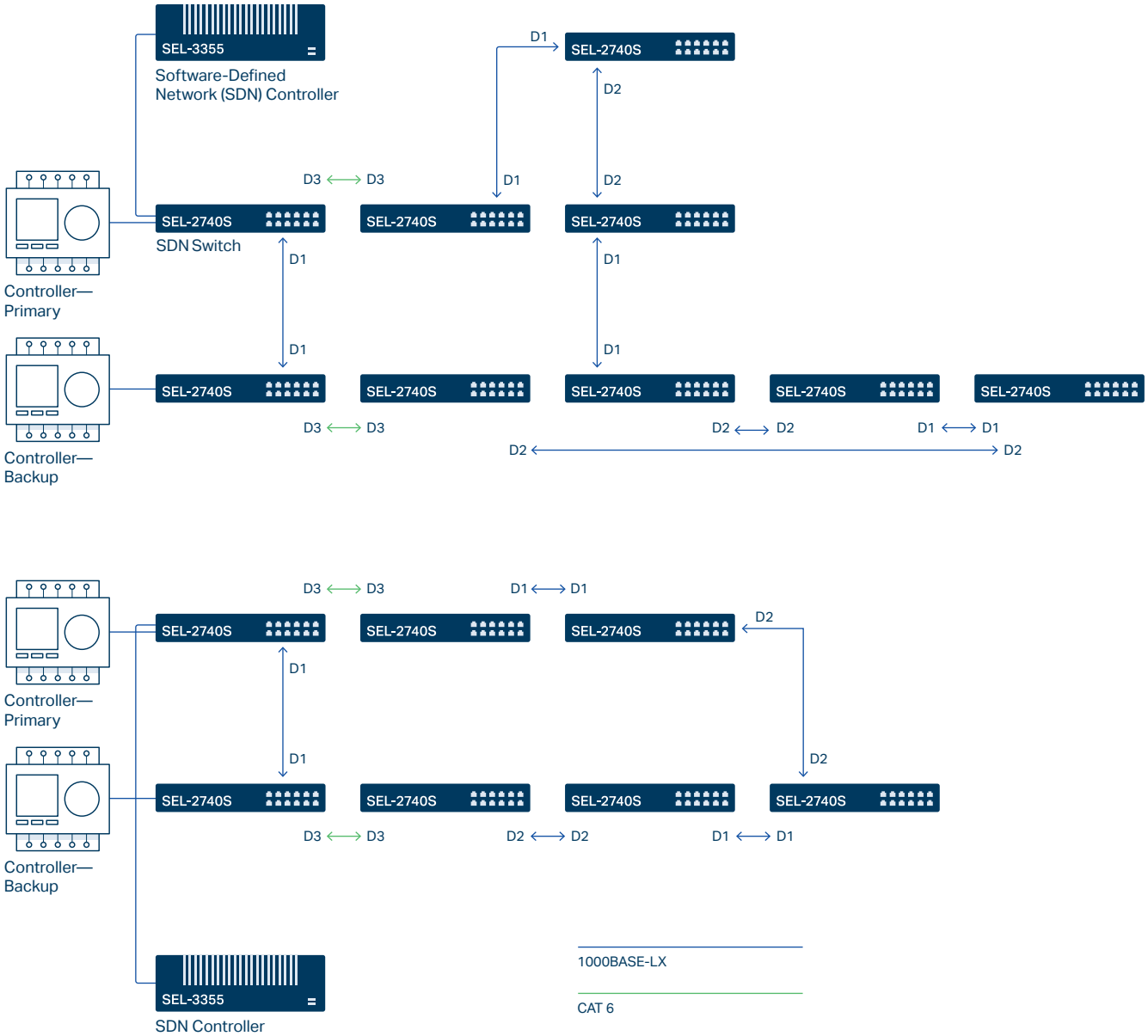

Figure 2—Proposed first solution

Implementation

As described by Jason Dearien and Tim Watkins in their recent white paper, "Migrating an Existing Network to OT SDN," one critical aspect required when migrating from a traditional network to an SDN network is "knowing everything" [1]. This can often pose a significant challenge when networks are poorly defined and lack documentation or when the networks have grown organically without a specified change management process. For New Indy, knowing everything presented a challenge. While some drawings were available, they were not entirely accurate and only limited information was known about the data flows. Additionally, the New Indy network team was busy supporting normal plant operations and maintenance and did not have the time to embark on the detailed fact-finding mission that the upgrade would require. To mitigate this issue, New Indy chose to enlist the help of SEL Cyber Services.

SEL Cyber Services network engineers specialize in the design, documentation, testing, and implementation of complex networks. To ensure consistent quality, SEL engineering projects follow a standard execution strategy, which includes detailed documentation and testing that includes a functional design specification (FDS), factory acceptance test (FAT), and site acceptance test (SAT). This ensures that the solution is documented, scalable, and tested before implementation.

Discovery Phase

The discovery phase of an SDN network upgrade begins by gathering all the existing network drawings, IP addresses, and data flow information. The SEL and New Indy network team's review of the network information revealed inconsistencies in the existing documentation. Knowing that documentation was limited, the SEL project plan included a pre-FAT site network validation visit and customer training. This proved to be vital to the success of the project as it enabled New Indy network engineers and SEL engineers to validate the network host and the required data flows for a successful SDN implementation.

Design and Configuration

SEL engineers created an FDS that specified the security controls to be leveraged in the SDN network, the new SDN network architecture, the network programming methodology, and the data flows between hosts. The new SDN architecture drawings were developed using the SEL Network Builder tools. The SEL Network Builder tools allow users to build their network settings from Microsoft Visio drawings, which ensures that the relationship between the drawings and the network configuration is always one to one. Additionally, it was decided that logical connections would be used for the network programming methodology. Using logical connections gave New Indy the flexibility to update the network settings from the flow controller if needed or use the API interface and Network Builder toolset, or both.

Network Validation and Training

Upon New Indy approval of the FDS and initial drawing sets, SEL engineers traveled to the New Indy site to validate the SDN configurations pre-FAT. This onsite validation of the network settings occurred during a maintenance period; however, SEL was not able to take any devices offline (i.e., remove their connection to the network) due to operational concerns.

During the SEL investigation of the network, it was discovered that only two managed switches existed, one for each network. This made it extremely hard to validate the SEL-created network design. However, through cable following, ARP scans, and Wireshark captures from the one SEL-2730M Managed 24-Port Ethernet Switch on each network. SEL assessed that the network settings were at an approximate 90 percent confidence level and that the modified network design was reasonably close to the existing network topology on everything except for host-to-switch connections, which were obfuscated by the panels. Each part of the investigation provided a different piece of information that was needed to create the final drawings and data flows:

- Cable following confirmed end device information, including the number of end devices on each switch as well as their make and model information. This information was used to adjust the topology and remove an under-utilized switch, which was kept by the customer as a cold spare.
- For SEL relays, the front-panel user interface was used to verify IP and subnet information. This revealed several host configuration issues, such as duplicate IPs on two relays as well as default IPs on all hot spare relays.
- Through ARP scans, the SEL team was able to validate all responsive IPs on the network. The results of these scans were later used to validate that all hosts were accounted for in the updated SDN drawings.
- Wireshark captures allowed SEL engineers to validate protocols on the network. The only SCADA traffic captured was Modbus. The duplicate IP addresses were also present in the Wireshark capture, and SEL relayed this information back to New Indy, but it was decided to not modify the IP addresses during the current maintenance window and instead to plan this activity as part of the upcoming outage.

Prior to commissioning, SEL and New Indy collaborated to ensure that the New Indy network team had a baseline understanding of how to use, install, and maintain an SDN system. SEL Cyber Services provided two days of training at the New Indy offices, where SEL covered Ethernet fundamentals, SDN basics, SEL-5056 Software-Defined Network Flow Controller use, and SEL Network Builder tools for commissioning, maintenance, and auditing. The New Indy engineering team quickly recognized the benefits and ease of use of SDN and, through two days of hands-on training using the SEL-supplied toolsets and networking equipment, were able to gain a thorough understanding of the SEL network upgrade design and execution strategy.

Factory Acceptance Testing

A critical component to the SEL Cyber Services project execution strategy is the FAT. A network FAT typically includes validating the SDN configurations and security settings and ensuring all equipment meets the required standards before site delivery.

With the information collected during the site visit, SEL adjusted the SDN topology and data flow diagram. The new switches were adopted to their respective flow controllers, and SEL performed testing to validate the configuration met the data flows required for New Indy's system. The auditing of data flows is performed by using the SEL Network Commissioning Assistant tool. This tool consists of a client and server that enables network engineers to craft packets and send the packets as a stream to verify end-to-end data flow through the network.

Additionally, since the project deliverables included two SEL-3355 computers acting as the flow controllers, the SEL Cyber Services team hardened both computers to Center for Internet Security (CIS) Level 2 benchmarks. CIS publishes security benchmarks for securing operating systems; the Level 2 benchmarks are intended to provide the most secure configuration for sensitive environments. The recommended settings were applied using the local group policy on each flow controller and audited during the FAT using the CIS-CAT Pro tool. A detailed compliance report was provided to New Indy as an outcome of this testing.

Site Acceptance Testing

After a successful FAT, SEL was prepared to replace existing network switches and validate the new SDN setup onsite at New Indy. With the knowledge and preparation gained during the validation phase, a detailed SAT plan was developed to quickly replace the existing network switches and to identify which devices in the panels were connected to each switch during the planned annual outage.

Due to the inability to disconnect physical ports from the switch during the network validation phase, SEL performed a quick ARP scan on each Ethernet cable as it was disconnected from the unmanaged switch and, upon discovery of the IP address, connected that cable to the appropriate port designated on the SDN switch. SEL then configured a dedicated miss port on each network and monitored for traffic. A miss port is a spare port on a switch that is configured to monitor traffic that does not match any flow rule—traffic that would typically be dropped. This allows the network engineer to verify that each device communicates as expected and that any required data flows were not missed. After verifying the communications were correct, the SEL engineering team transitioned to a standby and maintenance mode to support the plant startup procedure.

Results

The transition to an SDN-based network significantly improved New Indy's network reliability and performance. Key benefits included:

- Enhanced Redundancy—The new SDN architecture provided multiple failover paths, ensuring continuous network availability.
- Improved Visibility—The centralized control plane of the SDN solution allowed for better monitoring and management of network traffic.
- Reduced Downtime—Since the implementation, New Indy has experienced no further outages due to network failures, leading to uninterrupted production and increased efficiency.

After installation, SEL provided one year of enhanced maintenance to help smooth the transition to SDN. During this time, SEL engineers supported the New Indy team with the addition of communications for several devices to the SDN network and some troubleshooting of ABB devices; however, no network-related communications issues were observed. When asked about his satisfaction with the new SDN network, Al Gill, the New Indy systems engineer, responded: "It's invisible. We don't even think about the network. It's just there."

Conclusion

New Indy's adoption of SDN technology transformed their network infrastructure, eliminating the frequent outages that plagued their operations. The partnership with SEL Cyber Services ensured that the network upgrade was performed within the time constraints required to meet New Indy's operational goals. This success story highlights the potential of SDN to enhance network reliability and performance in industrial environments. If your business faces similar challenges, consider exploring SEL SDN solutions to achieve greater network stability and efficiency.

References

[1] J. Dearien and T. Watkins, "Migrating an Existing Network to OT SDN," SEL White Paper (LWP0037-01), 2022. Available: selinc.com.

SCHWEITZER ENGINEERING LABORATORIES

info@selinc.com	selinc.com	+1.509.332.1890	20250512