SDN Advantages for Ethernet-Based Control

Marcos Cabral, Mauricio Silveira, and Ryan Urie
Schweitzer Engineering Laboratories, Inc.

Introduction

There are many options available for interconnecting Ethernet networks. However, interconnecting operational technology (OT) networks that use Ethernet-based control presents unique challenges. For example, managing and optimizing the flow of IEC 61850 GOOSE messages (high-priority multicast messages for peer-to-peer communication) across networks requires precise engineering on traditional networks that use Rapid Spanning Tree Protocol (RSTP).

This white paper examines the benefits of using software-defined networking (SDN) technology to easily interconnect and manage traffic on OT Ethernet networks that communicate using IEC 61850 technology. A case study from the Itaipu Dam in South America, one of the world's largest hydroelectric facilities, is used to illustrate these benefits [1].

SDN Overview

SDN was originally developed to manage information technology (IT) networks with large volumes of traffic and frequent network topology changes. However, it has more recently been applied to OT networks in substations and industrial controls systems with great success. Unlike IT networks, OT networks do not undergo frequent changes. And, while IT networks are dynamic and flexible, OT networks are responsible for critical processes and high-speed decision making, which demand a network that is much more predictable and deterministic. Table 1 compares the characteristics of these two networking environments.

Table 1 Comparison of Ideal IT and OT Network Characteristics

IT	OT
Frequent network topology changes	Purpose-engineered networks
Plug-and-play connections	Deny-by-default security
Unhampered connectivity	Whitelisted flows
RSTP for backup paths	Predefined failover paths
Intermittent services with short lifetimes	Constant services with long lifetimes

In traditional networking, the switches that forward packets also determine the network path to send those packets through, using protocols such as RSTP. In SDN, by contrast, the decision-making functions are removed from the switches and handled instead by a centralized SDN controller, which is software that makes all the decisions for the network. The switches, in turn, receive packet-forwarding instructions from the SDN controller. This enables them to focus solely on the physical forwarding of packets.

SDN allows users to predefine the primary and backup paths for every communications flow on the network from the SDN controller. As such, OT SDN networks can be engineered in much the same way that power systems themselves are. Each device knows in advance what to do in case of a network failure. Because there is no need to negotiate forwarding paths, as in an RSTP Ethernet network, there is almost no delay in forwarding packets when there is a failure, which speeds up recovery and minimizes packet loss.

With SDN, network designers can define different forwarding paths for different applications (e.g., engineering access, GOOSE, or SCADA). This allows them to prioritize critical traffic or even send it on a dedicated link. In a traditional Ethernet network, all applications use the same links,

which limits the aggregate bandwidth usage to that of the slowest link in the network. Because SDN can assign each application its own path, the entire network bandwidth can be utilized.

SDN switches use deny-by-default security in which all packets without a predefined and authorized path are rejected. Each communications path and packet type must be authorized in advance, which prevents unwanted or malicious traffic on the network.

The determinism and security of SDN provide the following benefits:

- Optimized network traffic management through the elimination of unnecessary traffic, prioritization of critical traffic, total control of network paths, and the ability to set bandwidth and data rate limits.
- Enhanced situational awareness, with the ability to monitor every data flow. This enables system owners to know in near real time what is happening on their network.
- Extremely fast failure recovery. Because backup paths are predefined, switches can reroute traffic as soon as a network fault is detected (typically less than 100 µs, versus 10–30 ms for traditional networks).
- Improved cybersecurity from the deny-by-default architecture and the ability to control every packet on the network. SDN also eliminates common attack vectors found in traditional networks, such as Address Resolution Protocol (ARP) cache poisoning, Bridge Protocol Data Unit (BPDU) spoofing, Media Access Control (MAC) tables, RSTP, and broadcast Denial of Service (DoS) attacks.
- More precise testing and documentation. Because each path is created explicitly, it is possible to check each one during commissioning and network testing (including the failover paths) and to document the complete set of paths, protocols, and applications.

For more details on the structure, function, and history of SDN networks, see References [2] through [9].

SDN by SEL

The SEL SDN solution consists of SEL-2740S Software-Defined Network Switch hardware and an SEL-5056 Software-Defined Network Flow Controller, which can be hosted on an SEL-3355 Computer, as shown in Figure 1, or an equivalent Microsoft Windows computer or server.

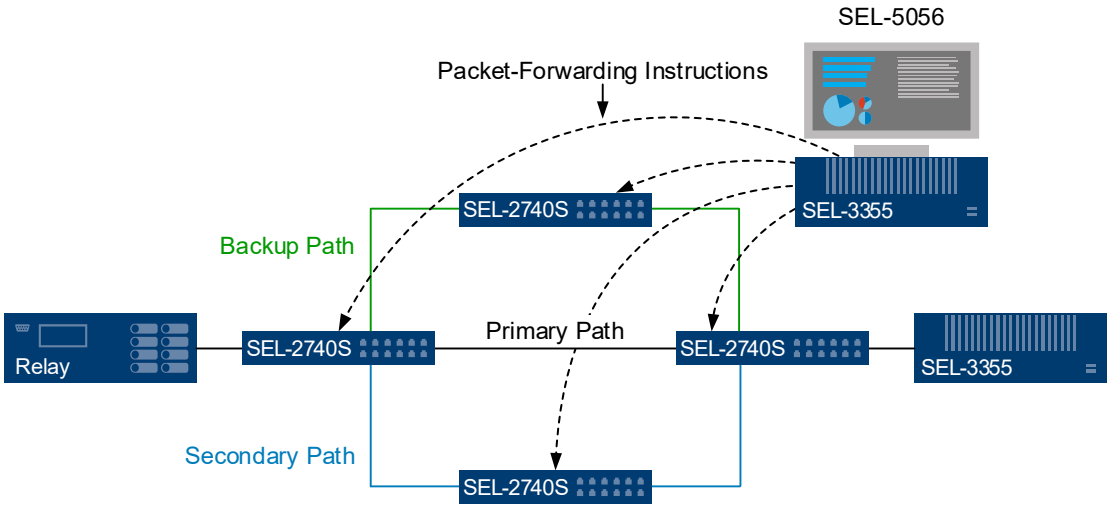

Figure 1 Basic SEL SDN Setup

After all the flow rules are configured in the SEL-5056 Flow Controller, they are sent to each SEL-2740S Switch with no interruption or outage. Once the rules are sent to each switch, the SEL-5056 can then monitor the connections and flows through the network.

The SEL-5056 Flow Controller proactively configures redundant paths not only to the primary path but also to the secondary path. This enables the SEL-2740S Switches to heal the network without needing to communicate with the SEL-5056. If the primary path fails, the SDN switches automatically transfer those data flows to the secondary path. If the secondary path also fails, they switch the flows to the backup path. This redundancy provides a high degree of network reliability.

The SEL SDN solution delivers high performance and reliability, simplified network management and testing, enhanced cybersecurity, and complete situational awareness.

Itaipu Dam Case Study

Interconnection Challenge

The Itaipu Dam spans the border of Brazil and Paraguay and is co-managed by the two nations. In 2016, it set a world record for energy produced by a single facility and is currently ranked only behind the Three Gorges Dam in China for overall generation capacity [10] [11].

Forced isolation protection (FIP) is a type of emergency control scheme at Itaipu. It uses panels at the Itaipu Dam Substation (FIP-01) and the Hernandarias Substation (FIP-02) about a mile away. The FIP-02 panel at Hernandarias Substation opens the interconnection between Itaipu and the National Electricity Administration (*Administración Nacional de Electricidad*, or ANDE) grid of Paraguay when there are undesirable variations in voltage and frequency or a reversal of the Itaipu-ANDE grid power exchange. Both substations communicate with an integrated industrial network system (*Sistema integrado de redes industriales*, or SIRI), an operations and control center for all of Itaipu's substations that is similar to a SCADA system. This scheme is shown in Figure 2.

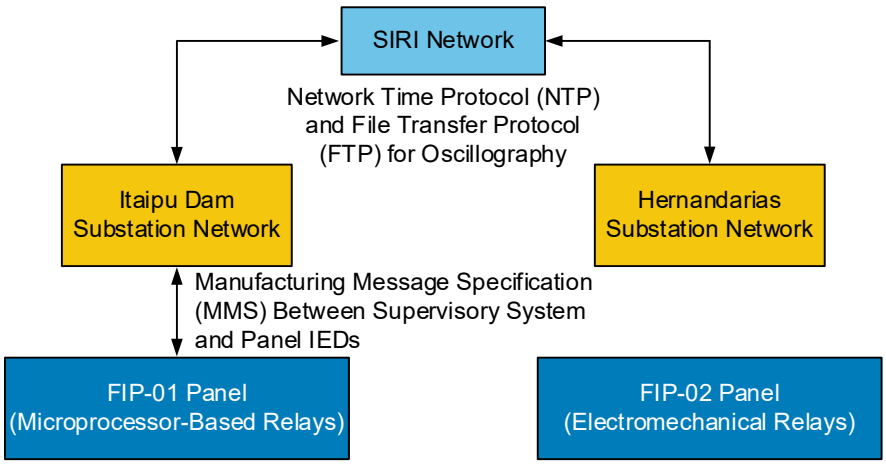

Figure 2 Initial Itaipu System

Itaipu engineers planned to upgrade FIP-02 from electromechanical relays to microprocessor-based relays that are IEC 61850-compliant to match those used in FIP-01. They wanted to connect the FIP-02 panel to the supervisory system through the Hernandarias Substation so that the FIP-02 relays could send Itaipu-ANDE power exchange levels to FIP-01 using GOOSE messages.

However, absolutely no configuration changes were allowed on FIP-01, including new VLANs, as such changes were considered too big of a risk for the large, in-service dam. The requirements for the new system are shown in Figure 3.

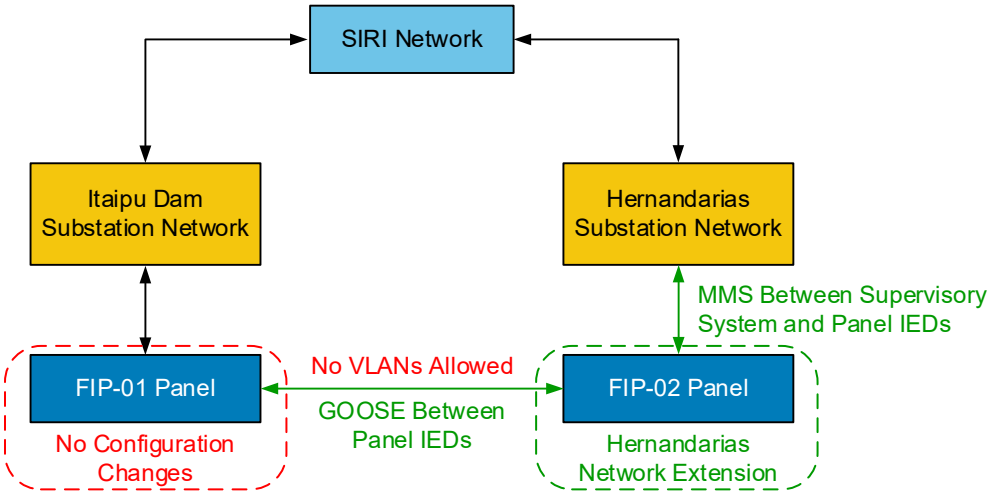

Figure 3 New System Requirements

Possible Solution: Independent RSTP Network for FIP-02

Directly integrating FIP-02 into the Hernandarias Substation network would have made the Itaipu system vulnerable to cyberattack, since the panel would give access to the plant network. Instead, the first option considered by Itaipu engineers to interconnect the FIP-01 and FIP-02 networks was to create an RSTP network extension for FIP-02, similar to the one at FIP-01.

In this scenario (shown in Figure 4), the FIP-02 relays would communicate with the supervisory system using MMS messages, communicate with one another using GOOSE messages, and communicate with FIP-01 using GOOSE and ARP messages.

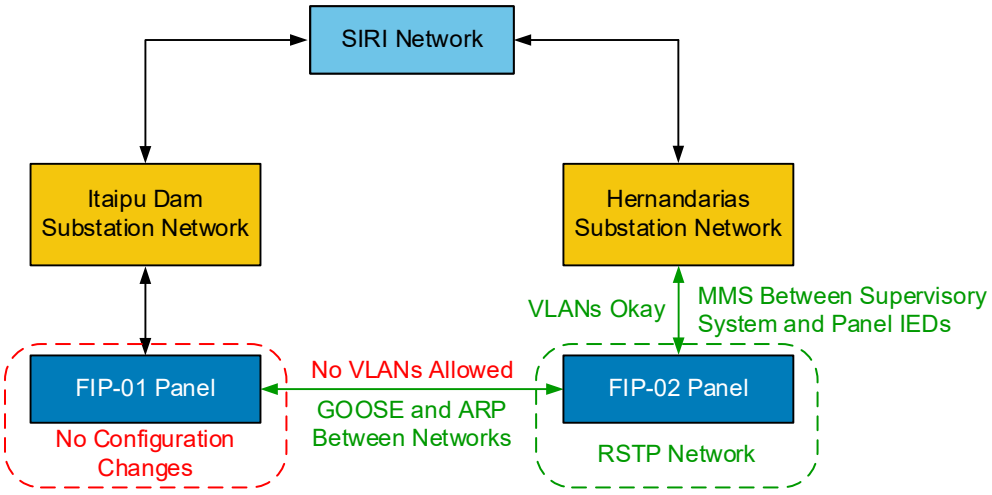

Figure 4 Independent RSTP Network for FIP-02 Panel

However, this option presented several network interconnection challenges due to the limitations of conventional networking technologies. Because the FIP-01 configuration could not change, there was no way to create new VLANs between FIP-01 and FIP-02 to control the GOOSE and ARP traffic and to prevent the formation of RSTP loops through SIRI. In addition, this option

increased the risk of packet loss due to high network reconfiguration and failover times and could have compromised cybersecurity because both substation networks would be accessible from the same point (FIP-02).

Moreover, any failure in the existing network caused by the interconnection with the FIP-02 network could compromise the plant's power line protection, an unacceptable situation.

Best Solution: SEL SDN for FIP-02

To overcome these challenges, the network designers decided to separate the logic of the FIP-01 and FIP-02 networks without altering the operation of the FIP-01 RSTP network. This was accomplished by using SDN technology to connect the two networks, with no change to existing network logic.

Figure 5 shows the system design. SDN switches in the FIP-02 network interconnect with FIP-01 by allowing certain GOOSE packets to be routed between the networks. The logical separation of the networks prevents ARP, BPDU, and GOOSE broadcast messages (flooding) between the networks and further prevents the formation of loops by forwarding only specific GOOSE messages.

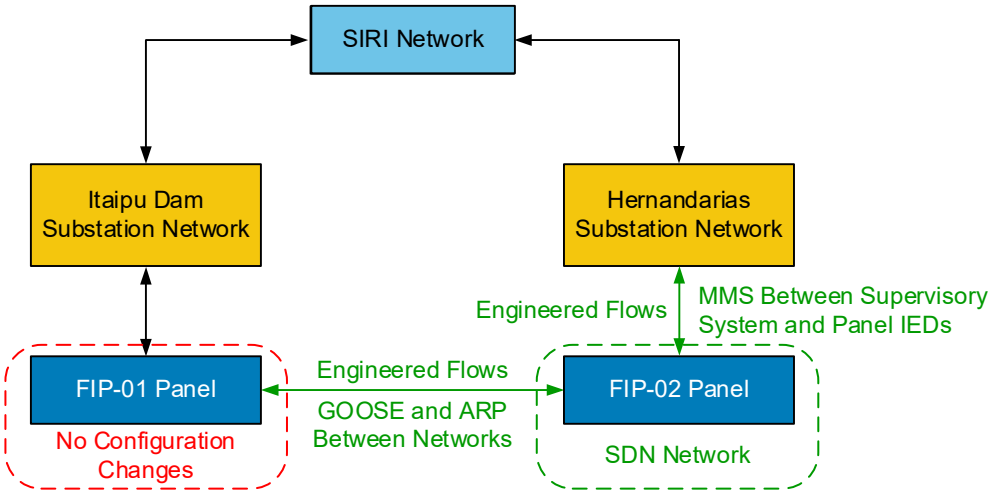

Figure 5 SDN Network for FIP-02 Panel

The SDN switches also added high levels of cybersecurity and enabled low network convergence times. While failover times are very important for GOOSE messaging, Itaipu's main reason for choosing SDN was to ease traffic management for their Ethernet-based control systems and to enable GOOSE connectivity between networks. The security and failover-time benefits were bonuses. The advantages of the SDN solution are summarized as follows:

- Control over GOOSE and ARP traffic.
- Elimination of loops.
- Fast failure recovery times.
- Reduced traffic management complexity versus RSTP.
- Tight control of GOOSE messages between the FIP-01 and FIP-02.
- Improved cybersecurity.

Because of these benefits and the simplicity of the SDN solution, Itaipu is now widely implementing SDN, even on new links where they could use VLANs for GOOSE messaging.

Network Engineering and Testing

Intensive network engineering was required to configure the SDN switches at FIP-02. Because SDN switches use deny-by-default security, network engineers had to fully predefine the communications flows of all system applications and carefully analyze the protocols used. In addition, they predefined secondary and backup paths in order to foresee all flows and paths. Because the data volume for configuring SDN switches is significant, the engineers had to carefully plan and document the configuration in detail.

The network engineers also fully tested the SDN system at the SEL factory using a platform that reproduced field conditions. They systematically tested each communication flow to ensure that all system applications functioned as expected. The network was tested under normal operating conditions and with simulated failures in the switches, the SDN controller connection, and the network links. In addition, the system cybersecurity was tested with intrusion tests using a port-scanning tool.

This testing demonstrated that it is possible to interconnect the FIP-01 RSTP network and the FIP-02 SDN network using GOOSE messaging without any modifications to the existing Itaipu Dam Substation network.

Conclusion

The interconnection between FIP-01 and FIP-02 has been in service since December 2018. This system is the first application of SDN technology in the Brazilian and Paraguayan electric sectors.

SDN technology made it possible to interconnect two Ethernet-based IEC 61850 networks without reconfiguring existing switches, and it simultaneously provided the system with high levels of cybersecurity and low network failure recovery times.

References

[1] P. Garcia, E. M. Nyznyk, M. A. Yamamoto, M. Cabral, M. Silveira, J. Chiaradia, B. M. Fontes, H. Larangeira, A. Insfrán, and D. F. Amarilla, “Application of SDN Technology in the Modernization of Part of the Schemes of Emergency Control of the 50 Hz Sector of Itaipu Binacional,” proceedings of the 14th Technical Seminar on Protection and Control, Paraná, Brazil, October 2018.

[2] P. Robertson, “Software-Defined Networking Changes the Paradigm for Mission-Critical Operational Technology Networks,” January 2017. Available: selinc.com.

[3] R. Hill and R. Smith, “Purpose-Engineered, Active-Defense Cybersecurity for Industrial Control Systems,” August 2017. Available: selinc.com.

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

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

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

[7] Q. Yang and R. Smith, “Improve Protection Communications Network Reliability Through Software-Defined Process Bus,” proceedings of the Power and Energy Automation Conference, Spokane, WA, March 2019.

[8] D. J. Dolezilek, “Using Software-Defined Network Technology to Precisely and Reliably Transport Process Bus Ethernet Messages,” proceedings of the 14th International Conference on Developments in Power System Protection, Belfast, United Kingdom, March 2018.

[9] N. Feamster, J. Rexford, and E. Zegura, “The Road to SDN: An Intellectual History of Programmable Networks,” *ACM SIGCOMM Computer Communication Review*, Vol. 44, Issue 2, April 2014, pp. 87–98.

[10] Itaipu Binacional, “Itaipu Had Its Best Year in 2016, With the Production of 103.1 Million MWh.” Available: www.itaipu.gov.br/en/press-office/video/world-record-2016.

[11] Z. Xin, “Three Gorges Project Reaches 1 Trillion kWh Milestone,” *China Daily*, March 2017. Available: www.chinadaily.com.cn/business/2017-03/01/content_28396395.htm.

Biographies

Marcos Cabral received a B.S. in electrical engineering from the State University of Campinas (UNICAMP) in 2008. He began working at General Electric as an automation engineer in 2008 and has been with Schweitzer Engineering Laboratories, Inc. (SEL) since 2010. He is responsible for training and customer support, configuration, factory testing, and commissioning. After ten years of experience with electric power system automation, Marcos is now a technical leader at SEL working on projects such as special protection systems, remedial action schemes, and the design and implementation of the software-defined networks. Marcos completed a specialization course in substation automation systems at the National Institute of Telecommunications (INATEL) in 2014.

Mauricio Silveira is an electrical engineer who received a B.S. from São Paulo State University in 2013. Since 2014, he has been with Schweitzer Engineering Laboratories, Inc. (SEL), where he has held positions in engineering services and sales and customer service, working in commissioning, factory testing, and customer support. He is currently an integration and automation engineer in R&D. His work includes the development and testing of protocols for critical applications, network design, cybersecurity assessment, and digital relay testing.

Ryan Urie received a B.A. in English from the College of Idaho in 2004 and an M.S. in bioregional planning from the University of Idaho in 2010. He joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2013 as a technical editor. In addition to editing numerous technical papers, application guides, articles, and presentations, he has authored several articles, white papers, and case studies.