# Software Defined Networking (SDN) Project

## Energy sector-focused SDN flow controller to manage control system networks centrally and securely

### Background

Traditional information technology (IT) approaches to network administration and packet delivery are not always appropriate for electric industry applications. The nondeterministic latency and configuration complexity make network design difficult for the deterministic, static control systems of the energy sector. In the electric industry, it is important to design the communications infrastructure to control device requirements and operational needs, and also account for redundancy to maintain reliability.

Electric industry control systems desire the ability to automatically identify and isolate affected network areas, re-route critical information, and control data flows with a deny-by-default cybersecurity policy. SDN advances cybersecurity by providing network access control while at the same time reducing the complexity. In addition, the size of field device firmware is greatly reduced, eliminating some patch management and configuration administration overhead.

### Barriers

- While SDN simplifies current packet structure and protocol requirements, it may cause interoperability issues with legacy network technology.
- Outreach and education will be needed to implement adoption of this new technology.

### Project Description

This project is developing an energy sector flow controller to be used with the SEL-2740S substation hardened switch, developed through the Watchdog Project. The SDN project is using standards based development to OpenFlow 1.3, which will be interoperable with OPENFLOW™ protocol-enabled network appliances. The SDN abstracts the network into three layers:

1) The **data plane** is the forwarding information base (FIB), or routing information base (RIB), that the switch uses to determine how to forward the packet.
2) The **control plane** learns the network topology and populates the FIB/RIB with forwarding instructions. The control plane decisions are centralized for easy administration and scalability. This centralized control plane technology is called a flow controller.
3) **Services** enable applications to be interfaced with the flow controller to harvest or present data to the controller and apply controls to the network(s).

Abstracting the control plane out of the data plane provides the network engineer with one place to view the network, design forwarding paths, and leverage future network services without downtime. In addition, the flow controller monitors, configures, and maintains safe, reliable network traffic flows.

### Benefits

- Establishes network access control with deny-by-default traffic engineering
- Improves the ability to identify deviations in network behavior as well as detect and analyze potential cyber intrusions
- Simplifies network configuration, reduces latency, and decreases incident response time
- Provides a global view of communication flows for improved situational awareness
- Proactively engineers network to all fault conditions eliminating the need for convergence algorithms like Rapid Spanning Tree Protocol (RSTP)
- Engineers traffic to the application and protects the transport performance requirements of the service

### Partners

- **Schweitzer Engineering Laboratories (SEL)**
- Ameren
- Pacific Northwest National Laboratory
- The University of Illinois at Urbana-Champaign (UIUC)

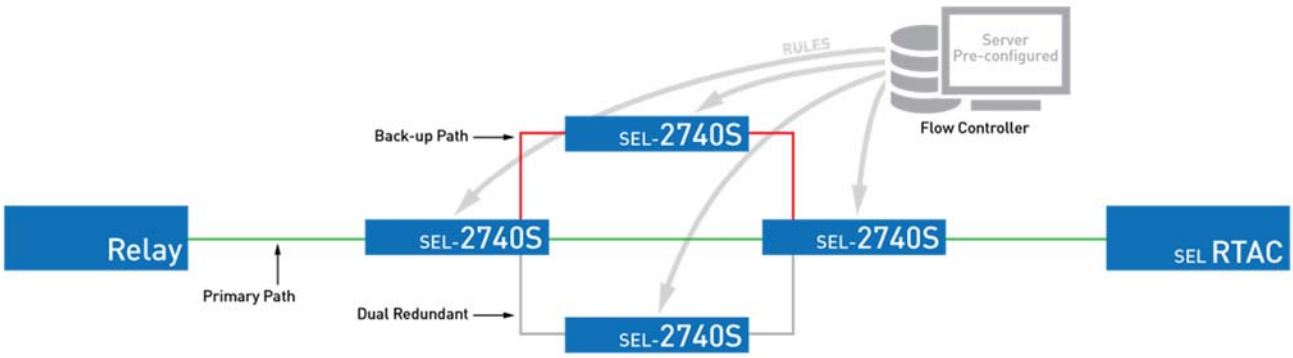


**Figure 1: SDN Applications**

## Technical Objectives

The project is developing a flow controller to be used with the SEL-2740S substation hardened switch. This project is using standards based development to OPENFLOW 1.3 to ensure interoperability with other SDN devices. The project team will test the SDN technology to ensure that it meets the high reliability requirements for the energy sector. All test results will be documented.

The final objectives of this project include:

- Introduce a more secure and highly reliable network technology than what is available today.
- Simplify the design, deployment, and management of more secure network technology to lower the total cost of ownership.

## Phase 1: Research and Development

- Research the best open-source controller to use as a foundation
- Identify industry benefits for SDN to be validated later in the project
- Develop the user interface, simplifying configuration for the flow controller
- Develop a flow validation application
- Commercialize a flow controller focused on the energy sector requirements for secure design, configuration, and monitoring of deployed field SDN technology

## Phase 2: End User Test Laboratory

- Test the technology in an asset-owner environment and document the results
- Run the technology through the procurement and validation process and document results
- Establish end user standards requirements necessary to safely deploy this technology on energy systems

## End Results

Project results will include the following:

- Energy-sector-specific SDN flow controller
- Documentation of best known methods for secure deployment of SDN in the energy sector
- Documentation of the benefits SDN provides over legacy switch fabric
- Flow validation application

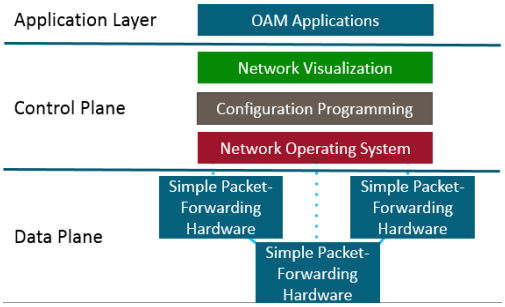


**Figure 2: SDN stack**

*Content last updated: May 2015*

**Cybersecurity for Energy Delivery Systems (CEDS)**

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Research and Development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of emergency disruptions due to cyberattacks.

**For more information:** https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

**Initial Leads**

Carol Hawk
Program Manager

Rhett Smith
Sr. Product Manager
Schweitzer Engineering Laboratories
509-336-7939
rhett_smith@selinc.com

**Current Contact as of Aug. 2020**

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov