SDN Project

December 23, 2016

Acknowledgment: This material is based upon work supported by the Department of Energy under Award Number DE-OE0000679.

Disclaimer: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Distribution: Unlimited Rights

Secure Control Systems for the Energy Sector

Funding Number: DE-OE0000679

Project Director:	Rhett Smith, SEL
Principal Investigator:	Joyce Sanders, Ameren
Principle Investigator:	Donald Borries, Ameren
Principle Investigator:	Rod Hilburn, Ameren
Principal Investigator:	Mark Hadley, PNNL
Principle Investigator:	Rakesh Bobba, OSU
Principle Investigator:	David Nicol, UIUC
Schedule Status:	**Completed**
Report Type:	Final Technical Report

Project Team:

Ameren
Pacific Northwest National Laboratories
Schweitzer Engineering Laboratories, Inc.
University of Illinois, Urbana-Champaign

Executive Summary

The SDN Project completed on time and on budget and successfully accomplished 100% of the scope of work outlined in the original Statement of Project Objective (SOPO).

The SDN Project formed an alliance between Ameren Corporation, University of Illinois Urbana-Champaign (UIUC), Pacific Northwest National Laboratories (PNNL), and Schweitzer Engineering Laboratories, Inc. (SEL).

The objective of the SDN Project is to address Topic Area of Interest 2: Sustain critical energy delivery functions while responding to a cyber-intrusion under Funding Opportunity Announcement DE-FOA-0000797. The goal of the project is to design and commercially release technology that provides a method to sustain critical energy delivery functions during a cyber intrusion and to do this control system operators need the ability to quickly identify and isolate the affected network areas, and re-route critical information and control flows around.

The objective of the SDN Project is to develop a Flow Controller that monitors, configures, and maintains the safe, reliable network traffic flows of all the local area networks (LANs) on a control system in the Energy sector. The SDN team identified the core attributes of a control system and produced an SDN flow controller that has the same core attributes enabling networks to be designed, configured and deployed that maximize the whitelisted, deny-by-default and purpose built networks.

This project researched, developed and commercially released technology that:

- Enables all field networks be to configured and monitored as if they are a single asset to be protected
- Enables greatly improved and even precalculated response actions to reliability and cyber events
- Supports pre-configured localized response actions tailored to provide resilience against failures and centralized response to cyber-attacks that improve network reliability and availability
- Architecturally enables the right subject matter experts, who are usually the information technology and operational technology engineers, to be the ones centrally administering the technology and responding to events
- Simplifies network configuration, improving deterministic Ethernet transport times, and providing instant visualization on where the communication circuits are and how all circuits are impacted when changes (e.g., configuration changes, failures or intrusions) happen, allowing operators to minimize downtime.
- Improves the ability to identify deviations in network behavior resulting in detection and analysis of potential cyber intrusions and faster response times

Results: This project has forever changed the way critical infrastructure networks are designed, secured, deployed and maintained. The cybersecurity and performance advantages achieved are significant, simply put traditional networking has been obsoleted while the team maintained Ethernet interoperability avoiding any legacy concerns. The team commercially released technology that accomplished all the cybersecurity goals outlined in the SOPO and completed it by executing the project management plan approved in the initial contract. The resulting Energy sector SDN flow controller model number is SEL-5056 and can be freely downloaded from the www.SELinc.com website. This technology not only improves the cybersecurity of control systems but has measured results that it improves the performance and reliability of the control system as well. This means the system owners can confidently apply it to their systems

knowing that it will, “first do no harm” but actually improve the system as well. Success of the project is best measured by the sales and deployment of the technology. System owners in industrial, electric, defense, and oil and gas only months after commercial release have approved plans for deployment.

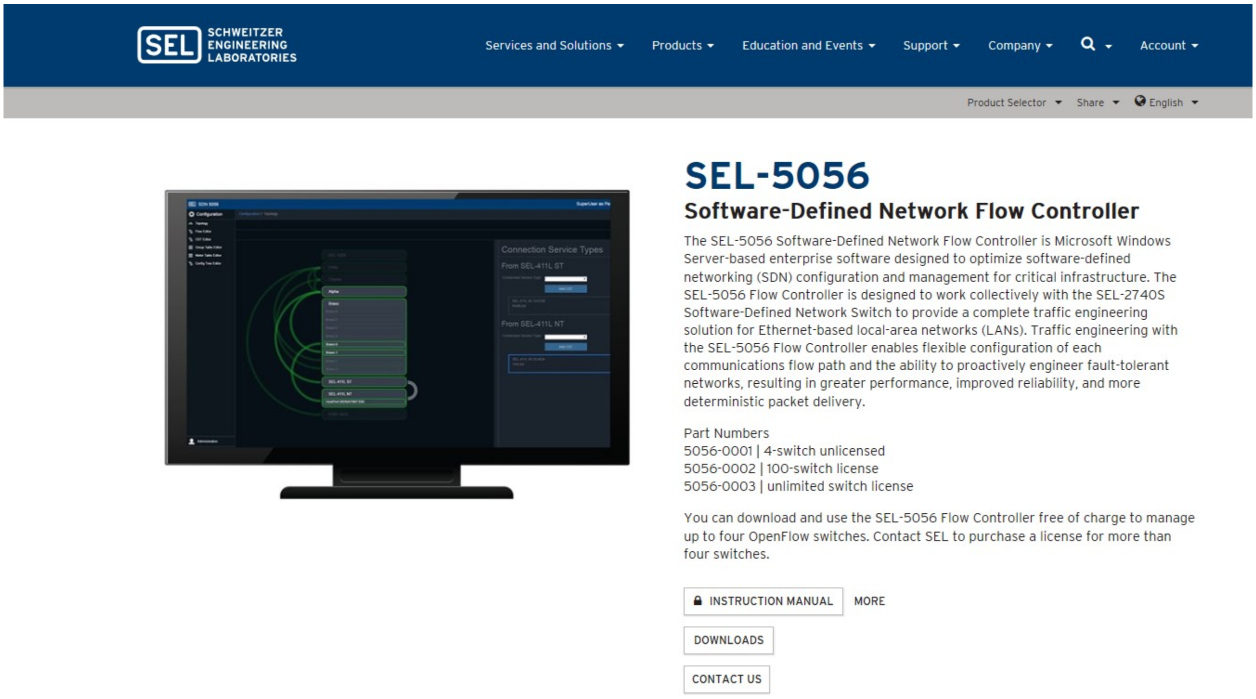
SOPO vs Actual Accomplishments

The SDN Project did not alter from the original approved SOPO and was able to successfully complete all milestones and deliverables on time and on budget over the three year period of the contract. This was accomplished through teamwork of all contract participatants and leadership by the experienced principle investigators. Below is a copy of the approved SOPO for the SDN project with the results detailed under each section.

A. Objectives

To develop a Flow Controller that monitors, configures, and maintains the safe, reliable network traffic flows of all the local area networks (LANs) on a control system in the Energy sector.

Results:
The SDN Project team lead SEL completed the development and commercially released the SEL-5056 with the research input from UIUC and PNNL design support and with successful validation testing from Ameren. This product can be found on the SEL website and the commercial flow controller software can be downloaded direct from this site



SEL-5056

Software-Defined Network Flow Controller

The SEL-5056 Software-Defined Network Flow Controller is Microsoft Windows Server-based enterprise software designed to optimize software-defined networking (SDN) configuration and management for critical infrastructure. The SEL-5056 Flow Controller is designed to work collectively with the SEL-2740S Software-Defined Network Switch to provide a complete traffic engineering solution for Ethernet-based local-area networks (LANs). Traffic engineering with the SEL-5056 Flow Controller enables flexible configuration of each communications flow path and the ability to proactively engineer fault-tolerant networks, resulting in greater performance, improved reliability, and more deterministic packet delivery.

Part Numbers
5056-0001 | 4-switch unlicensed
5056-0002 | 100-switch license
5056-0003 | unlimited switch license

You can download and use the SEL-5056 Flow Controller free of charge to manage up to four OpenFlow switches. Contact SEL to purchase a license for more than four switches.

B. Scope of Project

The Recipient will develop a Flow Controller that monitors, configures, and maintains the safe, reliable network traffic flows of all the local area networks on a control system in the energy sector. The project will produce the first solution system operators can use to view and configure geographically dispersed substation networks in their entirety as a single entity, taking the complex nature of the interconnected networks and providing a method for structuring and maintaining order. Operators will have the ability to engineer all the virtual circuits every communication flow travels on; pre-configure response actions to events; monitor communication flows; and react to undesired behavior to keep the critical systems operational. The technology will provide to operators a quick visual representation of what is happening, any communications that are impacted, and how they are affected. The Flow Controller provides an enterprise software solution to simply manage and monitor the health of all field networks, providing monitoring and visualization tools, configure field Network access control (NAC); verify that NAC configurations satisfy security and compliance policies; define specific actions to take on any new communication flow attempts; provide a monitoring window into what traffic is on each network and the flow circuits; establish central management capabilities for whitelisting protocols, applications, and devices on field networks; and configure automated defensive measures based on network behavior. This project builds on the current CEDS Watchdog project that produced a software-defined switch.

Results:

The SDN team completed the research, development and testing to validate the cybersecurity and performance advantages of the SDN technology and commercialized a flow controller tuned for the control system attributes of proactive traffic engineering purpose built systems with a deny-by-default whitelisted flow management approach. The one area the team was not able to commercial release was the automated methods for response to identified actions. The team did research and demonstrate the possibilities for this level of automation it did not make it in the first commercial release but is planned for many vendors to release this level of automation.

C. Tasks to be performed

The SDN project will be conducted in two primary phases. Phase 1 is the development and laboratory testing of the flow controller and flow visor. Phase 2 involves field-testing and involves creation of best practice and industry benefits documentation. Specific tasks for each phase are described in more detail, as follows:

Task 1.0: Project Management & Planning: The Recipient will revise the version of the Project Management Plan that was submitted with the application by including details from the negotiation process. The Project Management Plan will be updated as the project progresses and the Recipient will use this plan to report schedule and budget variances.

Results:

Completed and approved shortly after award, below is a table of the milestones with their planned completion and actual completion documented.

Phase 1 Research and Development resulting in commercial release

Task 2.0: The Recipient will complete the research into the existing flow controllers and perform the end user interviews to identify lessons learned and capture all operational and business requirements. The Recipient will then design use cases to capture the ways that the energy sector will use the technology so the rest of the project is steered by these use cases.

2.1: The Recipient will identify communications performance needs by collecting the control system communications requirements and overlay use cases (see task 2.4) to provide, expected results, fault cases, and failover considerations.

Successful Results:

The SDN team completed this task as a collective effort, all participated in collecting these requirements by collecting performance requirements from Ameren, critical control standards in IEEE and IEC, and many other Energy sector asset owners that SEL communicates with. These requirements were integrated into the functional and validation tests performed by the team to confirm the success of the technology before commercial release. The resulting performance measured far exceeded the teams expectations in three main areas; network healing, bandwidth efficiency, and disruptionless change management. The level of performance increase in this technology is significant and calls into question ever using the legacy Ethernet networking technology again.

2.2: The Recipient will verify open-source technology, leveraged from the existing flow controllers, Lemnos, and Padlock project, and the open-flow communities.

Successful Results:

The SDN team completed this lead by SEL and supported by UIUC but was not able to reuse any of the open source technology from these previous project but took the time to research if any other open source technology could be reused. The team did find open source test network tools, protocol stack libraries, and graphical user interface libraries that we were able to integrate that help insure interoperability success.

2.3: The Recipient will identify the industry benefits from testing, deploying, and operating an SDN network on an energy sector control system and write a white paper on the technical and economical benefits. The team will aim to present this white paper at an appropriate engineering technical conference to increase industry awareness and participation.

Successful Results:

The SDN team completed this as a collective effort, all participated in identifying many benefits of using the SDN technology over traditional networking and captured these benefits in the form of a datasheet, manual, and technical educational videos found on the SEL website under the SEL-5056 product page.

2.4: The Recipient will complete technical specifications for the flow controller and flow visor. The SDN team will complete specifications to integrate with the Watchdog Project.

Successful Results:
SEL completed this effort supported by PNNL and UIUC in their design reviews. The result is that the SDN Project commercial flow controller is the preferred controller for the Watchdog Project's SDN critical infrastructure network switch.

> 2.5: Research and develop technology to automatically verify that the flow rules specified in the controller (for both centralized, and distributed configurations, including network virtualizers such as flow visor) adhere to pre-specified operational, security, and compliance policies.

Successful Results:
UIUC completed this task supported by Ameren and SEL providing use cases and pass fail criteria. UIUC was able to demonstrate the ability to monitor the flows of traffic and validate them to the organizations network policies. This functionality is not currently in the commercially released flow controller but the research certainly paves the way for it to quickly be brought to market.

> 2.6: Research most reliable architecture of the flow controllers and network virtualizers (e.g., flow visor) for the most reliable fault tolerance system design and develop techniques to evaluate the resiliency provided by preconfigured backup routes and response mechanisms and suggest ways to improve resiliency.

Successful Results:
SEL lead this effort supported by Ameren and PNNL for operationally sound and security robust architectures including a solid method for testing, validation and deployment. The results were captured and integrated into the manual of the SEL-5056 teaching the industry how to use the powerful benefits of SDN for long term success.

> 2.7: The Recipient will author all uses cases that fulfill a utility partner's technical and business objectives for configuration, administration, and response actions desired for cyberattacks to keep the network communications operational while under attack.

Successful Results:
Ameren lead the identification of these use cases supported by SEL and PNNL to author them and convert them to design requirements in the technology development. The onsite validation testing at Ameren's Technology Application Center confirmed that these use cases were met.

> 2.8: The Recipient will complete the top level system requirements specification that combines the use cases and technical requirements. This document will lead the development of all software and hardware designs.

Successful Results:
SEL developed the SEL-5056 Flow Controller which is commercially released technology. This technology is backed by SEL's technical support, quality program, and industry sales and customer service support channels.

Task 3.0: The Recipient will develop the commercial flow controller and flow visor.

3.1: Perform all code reviews, static analysis, and protocol negative testing as well as all the functional and use case validation testing.

Successful Results:
SEL developed the SEL-5056 Flow Controller which is commercially released technology. This technology is backed by SEL's technical support, quality program, and industry sales and customer service support channels. PNNL also performed threat modeling and negative testing on the SEL-5056. The SEL team integrated the results into the development.

3.2: Perform code design based on the CEDS program Exe-Guard Project lessons learned.

Successful Results:
SEL developed the SEL-5056 Flow Controller in a way to take advantage of existing malware protective measures including the whitelist applications on the market maximizing the Windows platform instead of custom developing one for itself.

3.3: Complete network testbed development that will be used in testing and architecture and best practice research to validate the best architecture for the flow controllers and flowvisors.

Successful Results:
SEL completed the development of the technology testbed for long term support for the commercially release product.

3.4: Complete quality testing and software validation activities to the power system quality.

Successful Results:
SEL tests all products to Energy sector quality metrics and has commercially released the SEL-5056 flow controller and put all of its resources behind teaching, selling and supporting the technology for long term including having a robust roadmap for future enhancements. SEL has dedicated development teams planning to continue to work on this technology for the foreseeable future.

Task 4.0: The Recipient will complete robust laboratory testing that models the live system with a utility partner and demonstrate the commercial product in real-world control system installations and prepare best-practice guides for testing, deployment, and long-term management of the technology.

4.1: The Recipient will perform laboratory testing with a utility partner, academia partner, and national laboratory partner.

Successful Results:
All participants performed testing with successful results. SEL functional, unit, and validation tested the complete scope of the SEL-5056. UIUC completed testing of the flow validator. Ameren completed the end user validation testing at the TAC. PNNL completed the negative

testing and security architecture testing. All of these results have been captured and contributed to the publically released support literature in the manual for the product.

4.2: The Recipient will perform pilot testing with the partnered utility, academia, and national laboratory partners.

Successful Results:
Completed end user testing in a substation environment at Ameren in the TAC facility.

4.3: The Recipient will perform security robustness testing led by the partnering national laboratory.

Successful Results:
PNNL completed threat modeling and negative testing on the product and system level which then were fed back into the development at SEL.

Phase 2: Testing and Demonstration field deployment

Task 5.0: The Recipient will field test and demonstrate the commercial product in real-world control system installations and prepare a best-practices guide explaining how to test, deploy, and manage the technology for the long term.

5.1: The Recipient will perform field testing with the partnered utility, academia, and national laboratory partners, and demonstrate the product in a real-world control system installation.

Successful Results:
Completed end user testing in a substation environment at Ameren in the TAC facility. Ameren has on order the commercial released technology to be more permanently installed in the facility. The results were captured in the manual as the best practice guide.

5.2: The Recipient, with support from the utility partner and national lab partner, will author an industry benefits guide detailing the operational and economical savings realized from the end user perspective using the SDN network technology, as well as identifying all the cybersecurity advances this provides.

Successful Results:
Completed the best practice guides are the datasheet and manual of the commercially released product so all who use the technology benefit from this research and don't need to collect the results from another document.

SEL-2740S

Software-Defined Network (SDN) Switch

SEL-5056

SDN Flow Controller

Instruction Manual

20161122

D. Deliverables

Reports and other deliverables will be provided in accordance with the Federal Assistance Reporting Checklist following the instructions included therein.

In addition, the following deliverables are required to be submitted and shall be developed in accordance with written instructions provided by the DOE Project Officer.

Project Management Plan (PMP) Update – Due 90 days after award and resubmitted as necessary throughout the Performance Period.

Briefing/Presentation Materials - A copy of all briefing/presentation materials shall be provided prior to the event date.

Topical Reports – Due within 30 days after the completion of appropriate task

1. Topical report on SDN lessons learned and end user interview use cases captured. This report will also include the open-source protocols and standards that will be followed to achieve interoperable communications and a roadmap to multivendor interoperability.
2. Copy of Industry Benefits Guide white paper
3. Topical report on system functionality and specifications
4. Topical report on commercial product development and release
5. Topical report on the test plan and the pass fail criteria
6. Topical report on test results
7. Topical report on field testing and commercial release
8. Copy of best-practice guide

Successful Results:
All deliverables were generated and submitted in completion per the documented milestone delivery dates below.

MILESTONES	Planned Completion	Actual Completion
Project Starts	10/1/2013	10/1/2013
PHASE 1 | RESEARCH & DEVELOMENT		-
TASK 1.0 | PROJECT MANAGEMENT & PLANNING		-
Project Management Plan Updated	10/31/2013	10/30/2013
Deliverable | Updated Project Management Plan	**10/31/2013**	**10/2013**
Annual Project Briefing 1 (Kick-off Meeting)	*10/31/2013*	*12/11/2013*
TASK 2.0 | RESEARCH & DESIGN		-
Communication Performance Needs & Use Cases Identified	12/13/2013	1/2014
Open Source Technology Verified	10/30/2014	6/2014
Deliverable | Topical Report 1 - SDN Lessons Learned, Use Cases, and Open Source Protocols	**2/6/2014**	**2/2014**
Present Whitepaper Describing Technical & Economic Benefits	2/27/2014	4/2014
Deliverable | Industry Benefits Guide White Paper	**2/24/2014**	**4/2014**
Reliable Architecture, Fault Tolerance Technology & Resiliency Evaluation Techniques Designed	11/25/2014	5/2015
Flow Rule Auto-Verification & Auto-Generation Technology Prototyped	11/25/2014	9/2015
Project Briefing 2	*11/25/2014*	*3/2015*
Use Cases Authored	12/29/2014	10/2014
Top-Level System Requirements Specified	1/28/2015	3/2015
Technical Specifications Authored	2/25/2015	8/2015

Deliverable | Topical Report 2 - System Functionality & Specifications	**3/4/2015**	6/2015
Go/No-Go Decision Point 1	**3/4/2015**	**6/2015**
TASK 3.0 | COMMERCIAL PRODUCT DEVELOPMENT		
Commercial Flow Controller & Flow Visor Designed	4/22/2015	6/2015
Network Test Bed Developed	10/12/2015	9/2015
Preliminary Implementation of Flow Controller & Flow Visor Complete	10/12/2015	9/2015
Project Briefing 3	*11/9/2015*	*1/2016*
All Code Reviewed; Static Analysis & Testing Complete	1/12/2016	6/2016
Quality Testing & Software Validation Complete	3/8/2016	6/2016
Deliverable | Topical Report 3 - Commercial Product Development & Release	**3/15/2016**	**3/2016**
Go/No-Go Decision Point 2	**3/15/2016**	**3/2016**
TASK 4.0 | TESTING		
Testing & Demonstration Plan Written	4/5/2016	9/2015
Deliverable | Topical Report 4 - Test Plan & Pass/Fail Criteria	**4/12/2016**	**11/2015**
Laboratory Testing Complete	6/1/2016	9/2016
Field Testing Complete	7/28/2016	3/2016
Security Robustness Testing Complete	9/23/2016	9/2016
Deliverable | Topical Report 5 - Test Results	**9/30/2016**	**4/2016**
Go/No-Go Decision Point 3	**9/30/2016**	**8/2016**
PHASE 2 | DEMONSTRATION		
TASK 5.0 | FIELD TESTING & DEPLOYMENT		
Field Testing & Demonstration Complete	9/26/2016	6/2016
Commercial Product Released	10/7/2016	9/2016
Deliverable | Best-Practice Guide	**10/31/2016**	**9/2016**
Project Briefing 4 (Project Closeout Review)	*10/31/2016*	*9/2016*
Project Complete	10/31/2016	9/2016

Project Activities

The first key to success is to capture the right idea for the right problem use case. The SDN Project was a follow on idea from the DOE CEDS Project named the Watchdog Project which researched and developed the world's first industrial SDN switch. SEL and PNNL were already partnered for this project and saw an opportunity to apply the results of that project to address more of the cybersecurity roadmap and put the programmable network SDN establishes to provide network access control and planned responses to keep the system operating while under attack.

The second key to success is to collect a capable team. The SDN Project was a collaboration of four organizations; SEL, University of Illinois Urbana-Champaign, Ameren, and PNNL.

Collaborators: SEL is the world's leader in microprocessor-based electronic equipment for protecting electric power systems. Information Trust Institute (ITI) is a campus-wide research unit at the University of Illinois led by the College of Engineering that provides national leadership combining research and education with industrial outreach in trustworthy, secure, and reliable information systems. Ameren is a Fortune 500 company employing over 9000 people providing service to 2.4 million electric customers and more than 900,000 natural gas customers across Illinois and Missouri. PNNL performs basic and applied research to deliver energy, environmental, and national security for our nation. With this combined expertise and experience, we can effectively and completely accomplish our objectives and deliverables with a combined methodology of laboratory research and testing and product development with a goal of cost-effective commercialization of network communications security solutions.

A two phase project was executed, requiring a three-year period.

- Research, develop, test, and commercialize a control system flow controller, network virtualization device (e.g., flow visor), visualization tools, and design and configuration tools needed by system operators, and security protocols to secure all communications between these components that are specific to the energy sector control system networks
- Field test, and demonstrate the technology in real world control system installations and prepare best practice guides for testing, deployment, and long term management of the technology

The SDN project researched, developed, tested, and released the following:

- Flow controller tuned to the operational requirements of the energy sector
- Build on open source code as much as possible and perform interoperability tests with open source flow controllers and the SDN Project flow controller
- Configuration tools in the flow controller to enable operators to visualize the circuit paths their communications are traveling on and what happens in the event of a fault or attack to redirect the traffic away from the event and on to the intended destination.
- Research tools to automatically check that the flow rules specified in the controller adhere to pre-specified operational, security and compliance policies.
- Technology and methods to secure the flow controller communications between the network appliances and the controllers themselves. This resulted in the world's first secure control plane eliminating vulnerabilities that have been present for decades in BPDU spoofing and ARP cache poisoning.
- Best practice guides for system architectures and administration processes to maximize performance, awareness, and security were published in the product manual

Outcome and Benefits: This project produced the world's first industrial focused flow controller commercially available. This solution enables system operators to view and configure the geographically dispersed substation networks in their entirety as a single entity. This takes the complex nature of the interconnected networks and provides a method for structuring and maintaining order. Operators have the ability to engineer all the communication flows and their physical paths, preconfigure response actions to events, monitor communication flows, and react to undesired behavior to keep the critical systems operational.

The SDN Project results in a system solution that improves the control system performance and reliability and at the same time greatly increases the cybersecurity, no more compromises. The performance is increased by every port being utilized, no longer are there blocked ports due to legacy convergence algorithms like spanning tree and the network heal times are now under 100 microseconds compared to traditional networking at 10 to 50 milliseconds. The cybersecurity moved from a forward by default with traditional networking to deny-by-default and only whitelisted flows are forwarded regardless of what packet shows up at the switch. It is also multi-layer inspection instead of only layer 2 traditional switching. Another huge cybersecurity advantage is the legacy switching technology has always had vulnerabilities in the control plane, this project released the very first time these vulnerabilities are mitigated and no longer does the network have BPDU spoofing or ARP cache poisoning vulnerabilities, the MAC tables are gone and there is no longer a need for BPDU as the network does not use spanning tree. It's a win-win, the performance and security benefit and the cost of the technology is the same as traditional networking. The team achieved strong network access control and methods to survive an ongoing attack by minimizing the attack surface and at the same time improving the reliability.

SDN Project team activities

The team pulled together for this project work very well together and the experience from each of the stakeholders was perfectly balanced between academia, national laboratory, end user, and manufacturer bring every stakeholder perspective together with a common goal. Our first activity was to capture the use cases and industry requirements. This was lead by Ameren and captured by SEL which in turn converted them to design requirements. SEL also reached out to other customer of their can constructed a good cross section of use cases from a variety of asset owners. PNNL and UIUC contributed based on their indepth research knowledge of the technology and industry to help polish the use cases. Once we were all organized and aligned in the vision and tasks before us we split into each organization to complete the tasks ahead of them. Primarily SEL to develop the commercial product, UIUC to research the flow validator and network policy enforcer to demonstrate the potential, PNNL for the security modeling threat assessment and negative testing, and Ameren to coordinate with all stakeholders to continuously keep everyone end user benefit focused so we solve the right problems

Additional UIUC project activities

Senior Team Members: Rakesh Bobba, Roy. H. Campbell, Sibin Mohan, David M. Nicol, Faisal Hasan

Summary: UIUC/OSU team worked on the following activities during the course of the SEL SDN Project

1. **Kick-off and Use-case Gathering:** Participated in project kick-off and in use-case gathering meeting at SEL
2. **SDN Controller Evaluation:** Along with project team, evaluated different open-source controller technologies for viability in this project. Specifically looked at Beacon, NOX, POX and FloodLight.
3. **SDN Benefits to Industry Whitepaper:** Along with project team, authored a white paper on the benefits of SDN to the industry.
4. **Flow Validation Technology:** A major portion of UIUC/OSU team effort was devoted to the design, evaluation and integration of a flow validation module. As the name indicates, the function of this flow validation module is, given a network

topology and the set of flow rules configured in the switches, whether the configured rules satisfy certain pre-specified reliability and security constraints. For example, a reliability requirement could be that every critical flow has a back-up failover path. In order to make the development and coordination manageable, it was decided that the flow validation module will be designed and implemented as a controller application utilizing the northbound API of the SDN controller that SEL has developed. UIUC/OSU team worked closely with the SEL Development team to understand the northbound API and design and implement the flow validation module accordingly. Even with this nice functional separation for the teams, it took many iterations and quite a bit of integration effort on both sides to demonstrate the flow validation technology with the SEL SDN Controller. While the flow validation module has not been released with the initial version of the controller, this work demonstrated how the centralized management and programmability provided by SDN technology can be used to improve reliability, security and performance of control systems.

Flow Validation Module Components

A topology discovery mechanism: Developed a modular software model for topology by pulling information from the controller API to enable verification of various use-cases. Currently, the team tested this with use cases such as back up paths and protection of flows.

A high-level software model for the Switch: Given the discovered topology, the flow validator needs to pull the flow rules from the physical switches and validate those against a set of predetermined security policies. Instead of applying the flow rules to the physical switches for validating them, the framework uses an abstract model of the physical switches that SEL is building. This model has been implemented with enough details to capture the exact nature of the SEL switches in terms of flow processing.

A flow validation algorithm: The flow validation algorithm is at the heart of the whole framework. At present, the algorithm can check whether the installed flow rules can satisfy the policy which mandates having a backup path for every primary flow. Currently, the team is working on extending this algorithm so that it can check few other use cases incrementally.

Algorithm to check resilience of backup paths on link/node failure: The team have developed an algorithm that can check if backup path exists on single link and/or node failure. The software also has the capability to recomputed alternate paths on link and/or node failure for certain network topologies.

Design of operational constraint validator: The team implemented software that can collect fine grained traffic/usage statistics from the switches and determine hotspots in the network. This software can be used to validate if certain flows satisfy operational constraints like bandwidth/delay. It can also be used to maximize the efficiency/utilization of the links/switches maintaining the operational constraints. For example, the software can raise alarms if the utilization of a link goes above 75% of its bandwidth.

Aspects of this technology were published in 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm).

5. **SEL SDN Controller Testing:** Given the need to integrate the flow validation technology using northbound API, UIUC/OSU team in effect acted as the first internal customer for the SEL SDN controller. Many issued cropped up and all identified issues were quickly addressed by SEL.

6. **Ameren Demo:** UIUC/OSU team participated at the Ameren Demo, presented the design and some of the functionality of the flow validator.

7. **Flow Update Consistency:** Apart from the flow validation technology, UIUC/OSU team also looked into the problem of inconsistencies during flow/configuration updates due to the distributed nature of the network. Specifically, UIUC/OSU team identified the issue of interflow consistency violation and proposed solutions to address the problem. This work was published in the 2015 IEEE Communications and Network Security (CNS) conference.

8. **Other Activities:** UIUC/OSU team also explored (i) the security of host and link discovery mechanisms in current SDN technology and OpenFlow protocol in general, and (ii) explored the possibility of providing end-to-end delay guarantees for improved reliability.

9. **Publications:**

   i. Rakesh Bobba, Donald R. Borries, Rod Hilburn, Joyce Sanders, Mark Hadley, Rhett Smith, "Software-Defined Networking Addresses Control System Requirements," SEL Inc. Whitepaper #20140423.

   ii. Weijie Liu, R. B. Bobba, S. Mohan and R. H. Campbell, "Inter-flow consistency: A novel SDN update abstraction for supporting inter-flow constraints," 2015 IEEE Conference on Communications and Network Security (CNS), Florence, 2015, pp. 469-478. (A prelimnary version of the above paper appeared at the NDSS Workshop on Security of Emerging Networking Technologies (SENT) 2015.)

   iii. R. Kumar and D. M. Nicol, "Validating resiliency in Software Defined Networks for smart grids," 2016 IEEE International Conference on Smart Grid Communications (SmartGridComm), Sydney, Australia, 2016, pp. 441-446.

SEL-5056 Product Features

Automatic Topology Discovery. Enables touchless commissioning and discovery of network appliances and hosts on the network through use of the SEL-2740S.

Simple Licensing. Allows selection from two volume tiers with a one-time licensing fee and an optional version assurance program.

Ease of Use. Simplifies complex settings by using application-focused design to construct each network according to the applications running on the network.

Holistic Network Visibility. Allows viewing and management of network appliances as a single asset. Automated network topology discovery allows for near real-time situational awareness.

Low-Latency Flow Setup. Establishes new flows fast with low-latency flow setup times.

Scalable Network Deployments. Manages small or large networks with a single SEL-5056 installation.

Secure Configuration. Provides situational awareness and strong cybersecurity through user-based access controls, encrypted communication, and detailed audit logging.

Syslog. Performs log management through syslog for centrally automated col-lection and redundancy.

Supported Operating System. Provides high-quality, service-focused performance with Microsoft Windows Server 2012 R2.

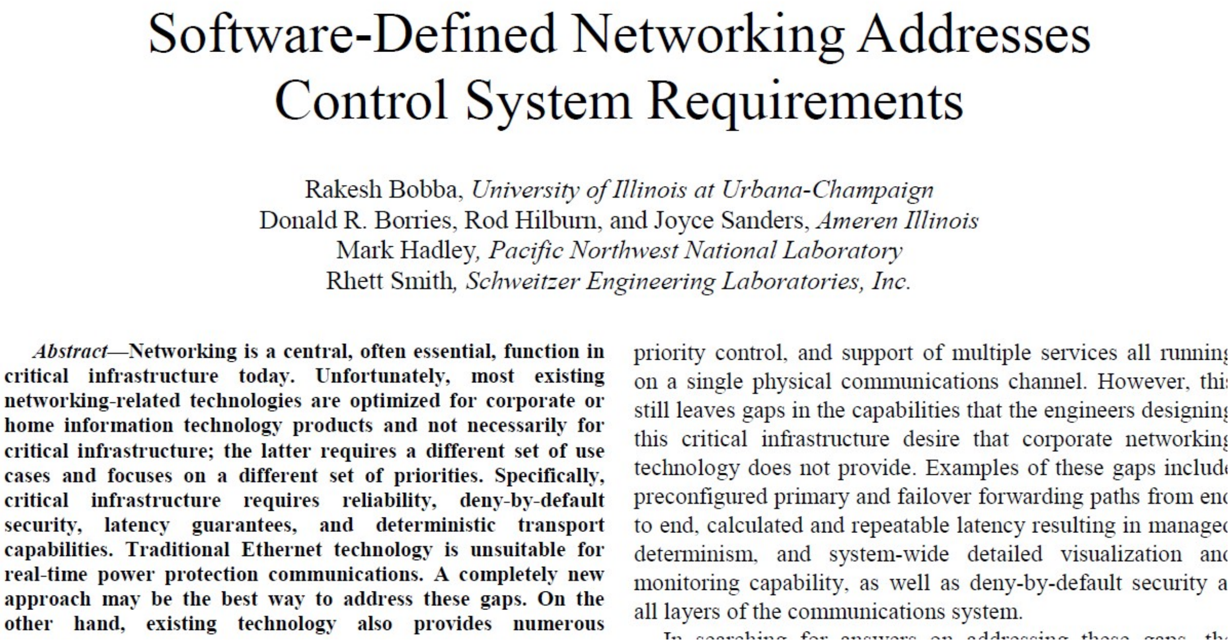
X.509 Certificate. Supports secure, mutually authenticated communication between the switch and the flow controller, and manages keys through X.509 certificates.

Central Authentication. Uses Lightweight Directory Access Protocol (LDAP) to centrally manage and authenticate authorized users.

Products Developed

The SDN Project Team completed the following products

1) Whitepaper documenting the benefits of SDN in the control system enviroment



Software-Defined Networking Addresses Control System Requirements

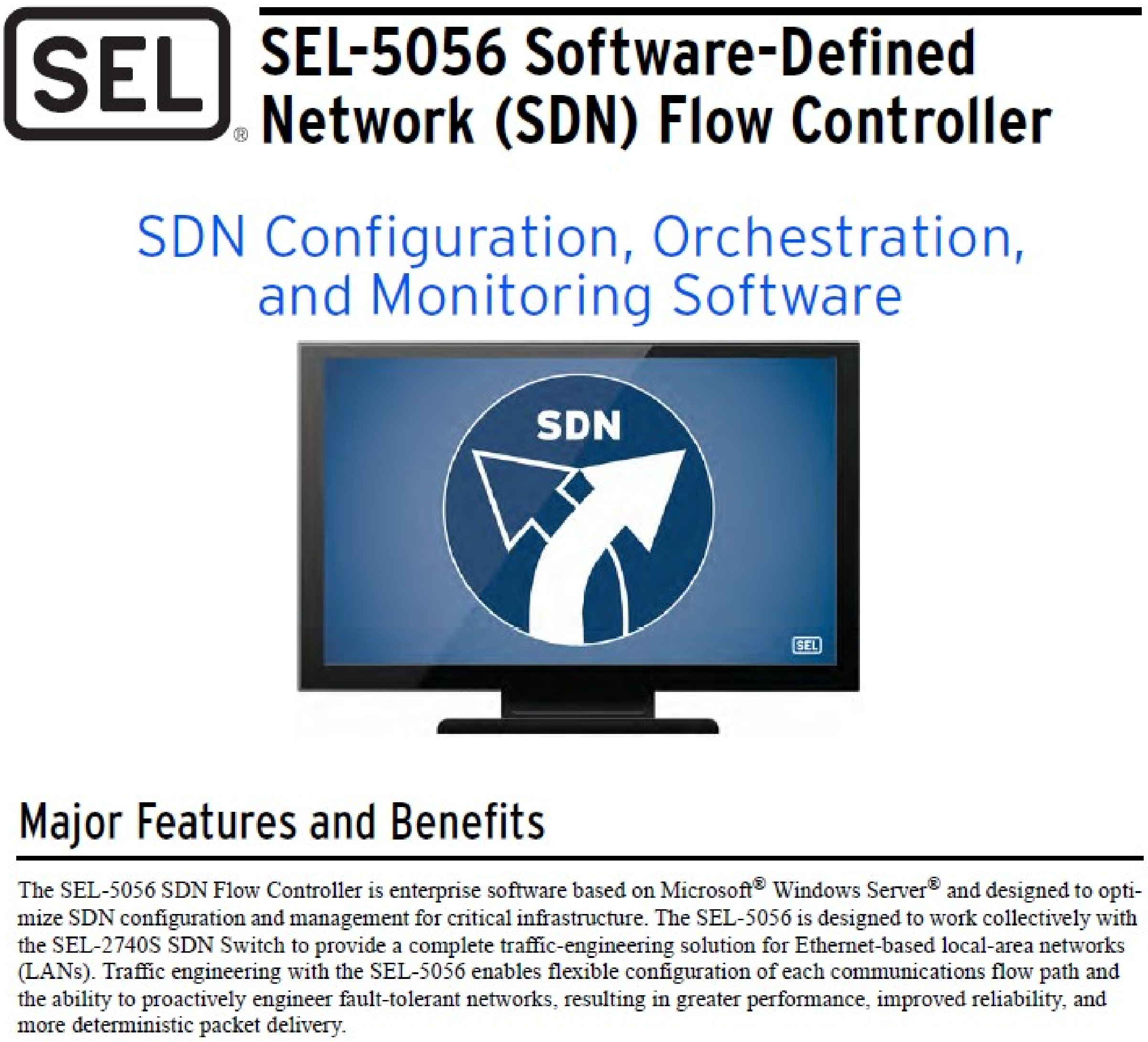
Rakesh Bobba, *University of Illinois at Urbana-Champaign*
Donald R. Borries, Rod Hilburn, and Joyce Sanders, *Ameren Illinois*
Mark Hadley, *Pacific Northwest National Laboratory*
Rhett Smith, *Schweitzer Engineering Laboratories, Inc.*

Abstract—**Networking is a central, often essential, function in critical infrastructure today. Unfortunately, most existing networking-related technologies are optimized for corporate or home information technology products and not necessarily for critical infrastructure; the latter requires a different set of use cases and focuses on a different set of priorities. Specifically, critical infrastructure requires reliability, deny-by-default security, latency guarantees, and deterministic transport capabilities. Traditional Ethernet technology is unsuitable for real-time power protection communications. A completely new approach may be the best way to address these gaps. On the other hand, existing technology also provides numerous**

priority control, and support of multiple services all runnin on a single physical communications channel. However, thi still leaves gaps in the capabilities that the engineers designin this critical infrastructure desire that corporate networkin technology does not provide. Examples of these gaps includ preconfigured primary and failover forwarding paths from en to end, calculated and repeatable latency resulting in manage determinism, and system-wide detailed visualization an monitoring capability, as well as deny-by-default security a all layers of the communications system.

In searching for answers on addressing these gaps, th

2) Commercially released SEL-5056 Flow Controller www.selinc.com/SEL-5056



SEL-5056 Software-Defined Network (SDN) Flow Controller

SDN Configuration, Orchestration, and Monitoring Software

Major Features and Benefits

The SEL-5056 SDN Flow Controller is enterprise software based on Microsoft® Windows Server® and designed to optimize SDN configuration and management for critical infrastructure. The SEL-5056 is designed to work collectively with the SEL-2740S SDN Switch to provide a complete traffic-engineering solution for Ethernet-based local-area networks (LANs). Traffic engineering with the SEL-5056 enables flexible configuration of each communications flow path and the ability to proactively engineer fault-tolerant networks, resulting in greater performance, improved reliability, and more deterministic packet delivery.

3) Industry best practice guidance on how to design and deploy this technology on critical infrastructure in the form of datasheet and manual for the SEL-5056

4) The research results have stimulated many dirivative work which include two more industry conference whitepapers, educational video tutorials, and industry 3-day educational hands-on class.
https://selinc.com/video/?vidId=116639
https://selinc.com/video/?vidId=116641
https://selinc.com/video/?vidId=117112

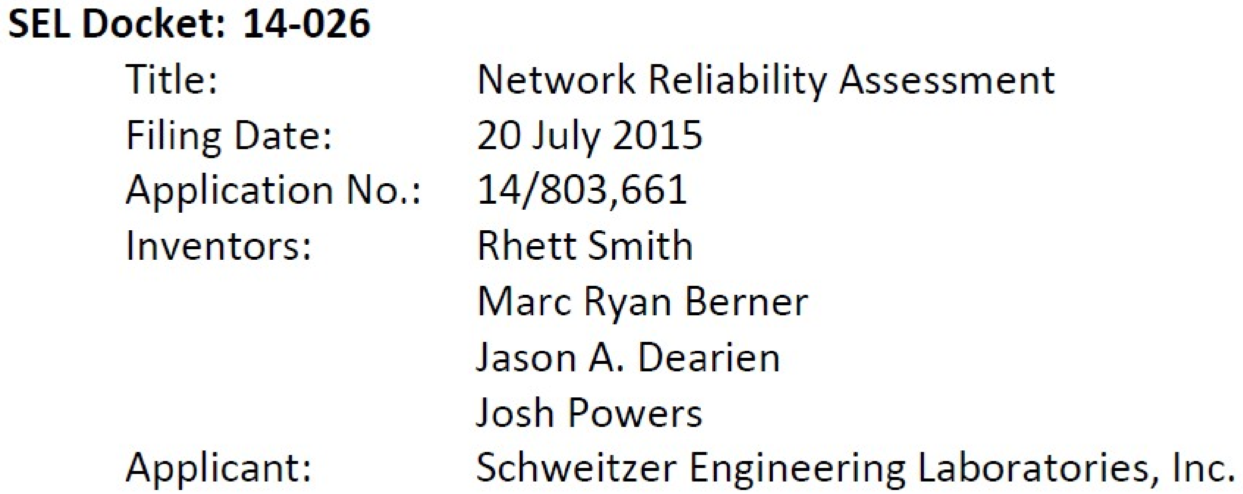
VIDEOS

HOW TO USE SEL-5056 SOFTWARE: INSTALLATION AND ADOPTION

HOW TO USE SEL-5056 SOFTWARE: ESTABLISHING LOGICAL CONNECTIONS

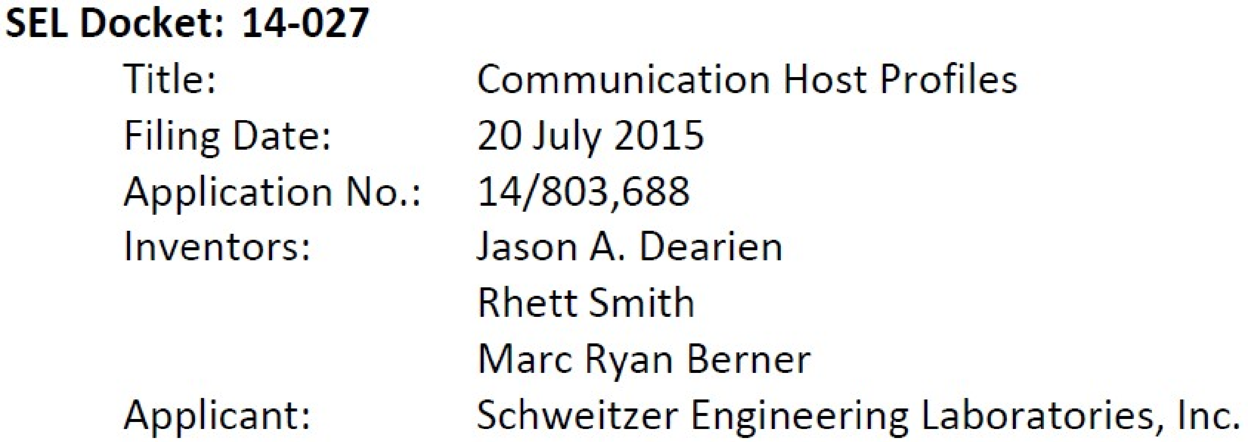
ENGINEER A BETTER NETWORK. IT STARTS WITH SDN.

5) Eight patents were filed under this project all lead by SEL. SEL submitted a report to DOE in compliance with 10 CFR 600.325



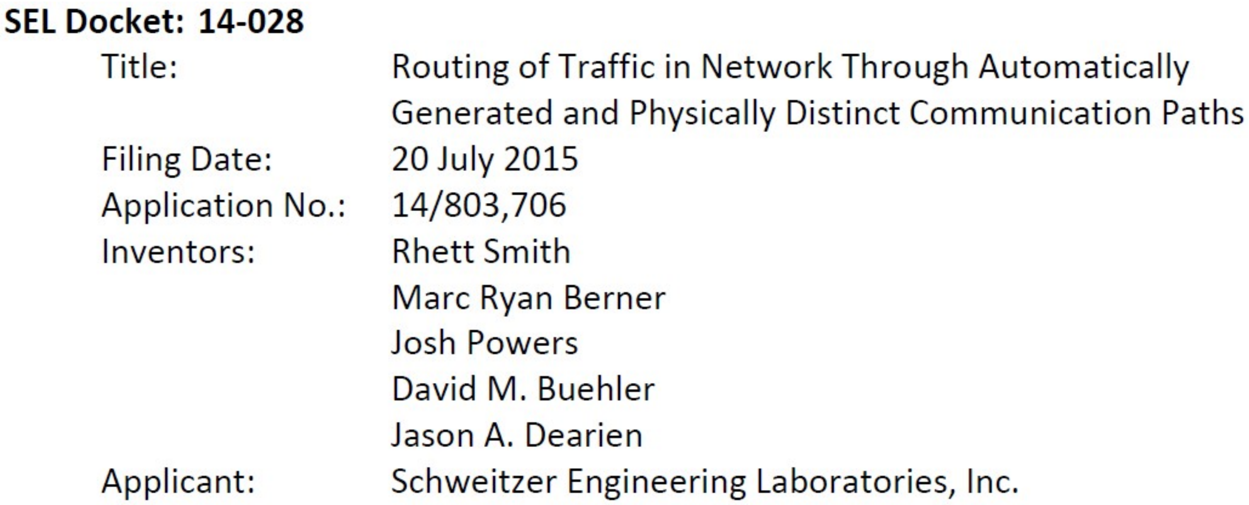
SEL Docket: 14-026

Title:	Network Reliability Assessment
Filing Date:	20 July 2015
Application No.:	14/803,661
Inventors:	Rhett Smith Marc Ryan Berner Jason A. Dearien Josh Powers
Applicant:	Schweitzer Engineering Laboratories, Inc.



SEL Docket: 14-027

Title:	Communication Host Profiles
Filing Date:	20 July 2015
Application No.:	14/803,688
Inventors:	Jason A. Dearien Rhett Smith Marc Ryan Berner
Applicant:	Schweitzer Engineering Laboratories, Inc.



SEL Docket: 14-028

Title:	Routing of Traffic in Network Through Automatically Generated and Physically Distinct Communication Paths
Filing Date:	20 July 2015
Application No.:	14/803,706
Inventors:	Rhett Smith Marc Ryan Berner Josh Powers David M. Buehler Jason A. Dearien
Applicant:	Schweitzer Engineering Laboratories, Inc.

SEL Docket: 14-029

Title:	Simulating, Visualizing, and Searching Traffic in a Software Defined Network
Filing Date:	20 July 2015
Application No.:	14/803,733
Inventors:	Jason A. Dearien Marc Ryan Berner Josh Powers
Applicant:	Schweitzer Engineering Laboratories, Inc.

SEL Docket: 14-031

Title:	Communication Device for Implementing Selective Encryption in a Software Defined Network
Filing Date:	20 July 2015
Application No.:	14/803,755
Inventors:	Rhett Smith Barry Jakob Grussling
Applicant:	Schweitzer Engineering Laboratories, Inc.

SEL Docket: 14-032

Title:	Communication Link Failure Detection in a Software Defined Network
Filing Date:	20 July 2015
Application No.:	14/803,773
Inventors:	Rhett Smith Marc Ryan Berner
Applicant:	Schweitzer Engineering Laboratories, Inc.

SEL Docket: 14-037

Title:	Configuration of a Software Defined Network
Filing Date:	20 July 2015
Application No.:	14/803,786
Inventors:	Marc Ryan Berner Rhett Smith Jason A. Dearien Josh Powers Grant O. Boomer
Applicant:	Schweitzer Engineering Laboratories, Inc.

SEL Docket: 14-038

Title:	Communication Device with Persistent Configuration and Verification
Filing Date:	20 July 2015
Application No.:	14/803,810
Inventors:	Barry Jakob Grussling Jason A. Dearien Ryan Bradetich
Applicant:	Schweitzer Engineering Laboratories, Inc.

Computer Modeling Involved

No computer modeling was produced in the SDN Project.

Conclusion

The SDN Project team completed all tasks in the SOPO in the originally approved schedule and budget. The result of the project is an industry changing performance and cybersecurity achievement pushing the reliability and security to the next level. System owners from many sectors have already identified the significant achievements accomplished under this project and are actively deploying it on their critical infrastructure. These sectors include Industrial where a paper mill is replacing all traditional networking devices to benefit from SDN, defense where bases are expanding their network to use this technology, oil and gas platforms for strict change control network enforcement, and electric industry in substation and generation networks. These asset owners have expressed their amazement in the major benefits this technology advances the reliability, network performance, cybersecurity, situational awareness and regulatory compliance. Success is when the industry benefits and uses the resulting technology of an R&D project, this team achieved success as many industries have voted with their wallets and purchased this technology only a short few months after commercial release with full intentions of system deployment to make their systems more reliable and more secure.