Watchdog Project

Dec 30, 2016

Secure Control Systems for the Energy Sector

Funding Number: DE-OE0000522

Project Director:	Rhett Smith, SEL
Principal Investigator:	Jack Campbell, CenterPoint
Principal Investigator:	Mark Hadley, PNNL
Schedule Status:	**Completed**
Report Type:	**Final Technical Report**

Project Team:

Schweitzer Engineering Laboratories, Inc.
Pacific Northwest National Laboratory
CenterPoint Energy Houston Electric

Executive Summary

The Watchdog Project completed 100% of the project Statement of Project Objective (SOPO). The Watchdog project was a very aggressive project looking to accomplish commercialization of technology that had never been commercialized, as a result it took six years to complete not the original three that were planned. No additional federal funds were requested from the original proposal and SEL contributed the additional cost share required to complete the project.

The result of the Watchdog Project is the world's first industrial rated Software Defined Network (SDN) switch commercially available. This technology achieved the SOPOO and DOE Roadmap goals to have strong network access control, improve reliability and network performance, and give the asset owner the ability to minimize attack surface before and during an attack.

The Watchdog project is an alliance between CenterPoint Energy Houston Electric, Pacific Northwest National Laboratories (PNNL), and Schweitzer Engineering Laboratories, Inc. (SEL). SEL is the world's leader in microprocessor-based electronic equipment for protecting electric power systems. PNNL performs basic and applied research to deliver energy, environmental, and national security for our nation. CenterPoint Energy is the third largest publicly traded natural gas delivery company in the U.S and third largest combined electricity and natural gas delivery company. The Watchdog Project efforts were combined with the SDN Project efforts to produce the entire SDN system solution for the critical infrastructure.

The Watchdog project addresses *Topic Area of Interest 5: Secure Communications*, for the DE-FOA-0000359 by protecting the control system local area network itself and the communications coming from and going to the electronic devices on the local network. Local area networks usually are not routed and have little or no filtering capabilities. Combine this with the fact control system protocols are designed with inherent trust the control system owners have very little choice on how to protect communications on the local network. The Watchdog project reduces security risks in electric sector control system local area networks (LANs) by providing:

Network access control (NAC)

Multi-Layer firewall (physical through transport layer)

Containment of malware or unauthorized traffic spreading across the network

White list protocols and application message types filtering

Configurable, proactive traffic engineering

The Watchdog project achieved all of the above by developing a SDN switch.

Control system communications are consistent and predictable in contrast to corporate network communications that are very dynamic and ever changing. The Energy sector can take advantage of this and develop technology that only allow known good communications and have a deny-by-default network access control security posture that requires very little management and can be scaled quickly and efficiently.

This project will improve operations and mitigate local area network risks by providing important tools to improve the ability to securely manage the control system LAN and the equipment connected to this LAN. These tools include:

Providing an application layer firewall to serve as a counter measures to newly discovered security vulnerabilities until firmware upgrades to primary equipment can happen in a safe, reliable, and economical manner.

Automating LAN resiliency through identification and reaction to unauthorized traffic providing containment of malicious traffic

Logging and reporting events and actions occurring at all layers of the network

Replicating switch configurations for a secure and trusted method for contingency planning or network appliance backup

This project supplies the Energy sector with control system hardened and tested equipment that will provide network access control and network defense solutions. Projects like the DOE funded Lemnos Project have provided solutions for perimeter defense for control systems. The Watchdog project in contrast provides the next layer of defense at the local network layer which moves one step closer to the end device. The resulting product can be integrated into both existing and new control system networks enabling the Energy infrastructure to improve uniformly without limitations due to protocols or vendor specific equipment requirements.

This project fulfills important milestones in both the DOE Roadmap to Secure the Energy Sector and the NERC CIP standards. The Watchdog project provides "widespread implementation of methods for secure communication in a scalable and cost-effective to deploy" which is a milestone identified in the DOE Roadmap. The Watchdog project also provides solutions for CIP-005 and CIP-007 by providing strong access control to the local area network and allows the asset owner to control what protocols, messages or commands, and what devices can communicate to other devices in a network. Ultimately this provides the granular change control tools needed to lock down and monitor the field control system networks to make sure they continue to stay in a known good state.

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 switch model number is SEL-2740S and its details can be viewed 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 The Watchdog team accomplished.

Phase 1:

- Identified the functional requirements at Utilities for a managed switch with multi-layer inspection and network access control. This task was used to develop the specifications of the commercial product, SEL-2740S
- Searched open source technology for functional solutions and identify interoperable opportunities for configuration and logging. This lead to the use of Open Virtual Switch (OVS) and the protocol OpenFlow.
- Identified hardware that supports the required communication speed and uphold the control system reliability needs.
- Authored the detailed specification of the hardware and firmware of the commercial product
- Designed the user interface and hardware interfaces of the commercial product
- Develop the commercial product, SEL-2740S

Phase 2:

- Lab tested the prototypes at Ameren to make sure the team is on track to accomplish all the technical and business
- Lab tested the prototypes at PNNL for security robustness
- Release of commercial product
- Watchdog team authored best practice guide explaining how to test, deploy, and manage the technology for the long term which are now all published on the SEL website in the form of manuals and datasheets.

The project team did identified the need to have central management of the new technology so requested and was approved a SOPO change to include the task to develop central management interfaces on the switch. This change ultimately lead to the integration of the Watchdog Project and the SDN Project to work as a unified project to release a system solution for the network access control security technology

The following are the specific tasks under the contractual Statement of Project Objectives (SOPO) with the results of the project team work identified below each task.

C. TASKS TO BE PERFORMED

Phase 1

Development of a managed switch that performs multi-layer packet inspection and provide network access control for the critical infrastructure.

Task 1.0 The Watchdog project plan will first be revised after the negotiation process between DOE and the Watchdog team is completed, to accurately reflect the milestones and deliverable timelines.

This was performed in a timely manner and the team started work immediately

Task 2.0 CenterPoint, SEL, and PNNL staff will complete the research into the local network communication load needs and develop all possible use cases for Watchdog technology. These use cases are the ways that the electric sector will deploy and use the

technology which will drive the specifications of the product. This can be broken into 3 subcategories

The Watchdog team completed this task with multiple conference calls and a face-to-face meeting where all team members met and discussed the details of each use case. The use cases where authored and circulated to each team member till all approved them. These use cases drove the technical scope and the functional priority.

Task 2.1 Identify communication performance needs. This will be done by collecting the control system communication requirements and overlay uses cases (see task 2.4) to provide worse case burden.

The team identified the strongest requirements where IEC61850-9-2 sampled measured values in the fact the network must heal from any network event in 624uS. The heaviest data load on the network is VoIP and video camera data with 20 to 30Mbps flows.

Task 2.2 Search open source technology for functional solutions and identify interoperable opportunities for configuration and logging. This can be broken into two sub tasks

Task 2.2.1 Select open source code that fulfills desired functionality

SEL lead this task and identified OVS as the open source library to use in the SEL-2740S

Task 2.2.2 Test open source code to determine if it works to the worst case burden

SEL tested in the identified use cases and have documented passing results for each being able to heal fast enough, pass enough data, and keep the latency and jitter to the levels needed.

Task 2.3 Complete hardware requirements specifications.

SEL designed, developed and tested to the hardware to protective relay standards for reliability IEEE1613 and IEC61850-3 with passing results.

Task 2.4 Author all uses cases that fulfill CenterPoint's technical and business objectives for a managed switch and the security requirements for protecting the local area network it runs on.

Completed by all the team

Task 2.5 Author the technical specifications for the hardware and software

SEL lead this effort and based them from the use cases

Task 2.6 Watchdog team 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.

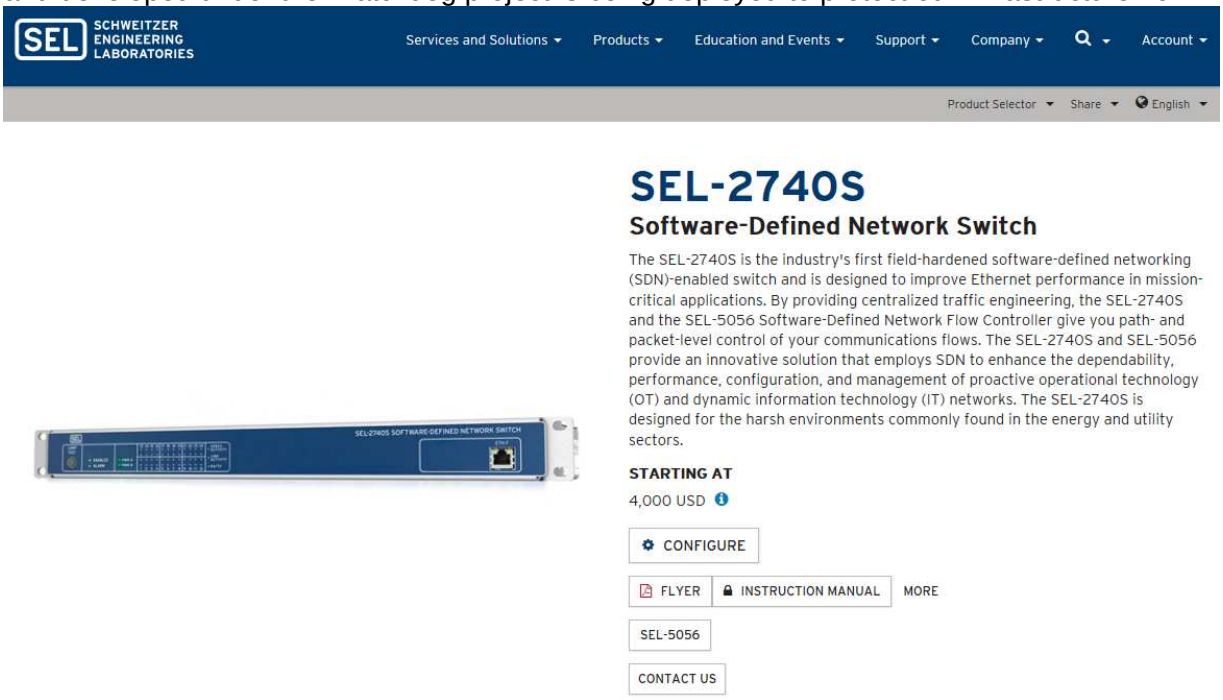
SEL lead this effort and based them from the use cases

Task 2.7 Design user interface control system environment

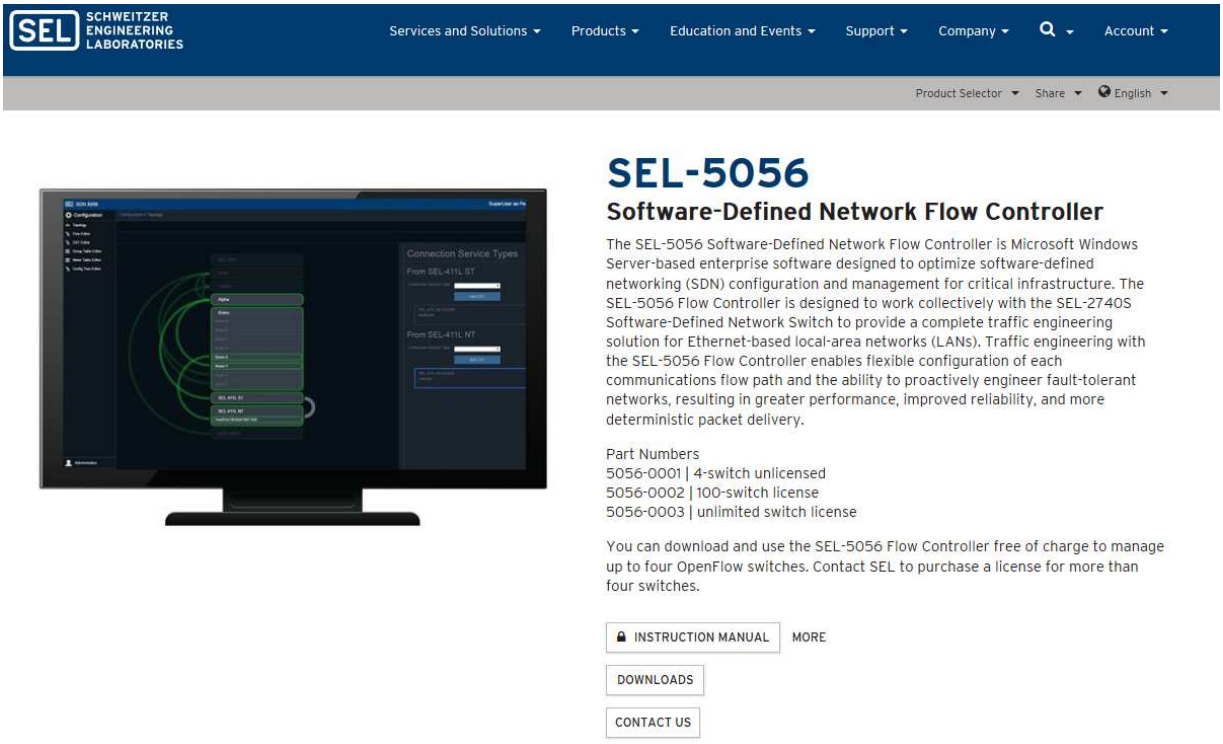
SEL lead this effort with lots of feedback from the project team to design the right tool for the operators

Task 3.0 Develop the commercial managed switch with multi-layer packet inspection

SEL lead this effort and developed the switch through the existing product development processes established at SEL. The result is that the SEL-2740S is commercially released and selling to critical infrastructure asset owners across the country. The technology researched and developed under the Watchdog project is being deployed to protect our infrastructure now.



Task 3.1: Network management software to centrally monitor and manage this technology
This task lead the the unification of the Watchdog and SDN Projects and this task was completed by developing the interface on the SEL-2740S to connect to the SEL-5056 flow controller central software to manage all deployed SEL-2740S as a single asset centrally.



Task 3.2 Hardware Prototype 1 and environmental testing complete.
SEL completed this prototype and tested it to identify all changes needed for proto two

Task 3.3 Hardware prototype 2 and environmental testing complete.
SEL completed this proto and tested it, unfortunately the second proto did not pass all needed hardware tests either so SEL had to spin proto 3.

Task 3.4 Complete remaining FW, HW, and SW development activities.
The Watchdog team completed all the development and released the SEL-2740S in September 2016

Phase 2
Lab test, field test, 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

Task 1.0 Perform robust lab testing that model the live system. During laboratory testing, the impact upon the control system will be measured. The environment will be monitored using a protocol analyzer to measure any impact the packet inspection is having on IED performance. In addition to performance, the impact on the operators of the control system will be identified. For example, are changes required on the IEDs to deploy the new technology? What configuration settings are required to support the technology? What are the cabling requirements and maintenance requirements? This information will be used as input for project deliverables.

The Watchdog team by this time had combined efforts with the SDN Project team and performed the testing at Ameren at their Technology Application Center (TAC). The team authored a test plan, executed that test plan and all tests where successful.

Task 1.1 CenterPoint Lab Testing

The team tested at Ameren with successful results

Task 1.2 CenterPoint Field Testing
After successful laboratory testing, CenterPoint staff will perform a field test. CenterPoint engineering staff will install the switches, identify lessons learned from an asset owner's perspective, and provide feedback to SEL and PNNL on the deployment.
The team was not able to have field performance testing in time of the project close due to the extended schedule it took to commercially release the product but there are many utilities across the nations currently designing and deploying the technology now with success.

Task 1.3 PNNL Security Robustness Testing

PNNL completed a threat modeling evaluation and presented findings to the team, SEL took those findigs and improved the design of the product. PNNL also performed indepth negative testing and presented those findings to SEL and SEL addressed them in the development team.

Task 2.0 Commercial product release

The Watchdog team completed all tasks, deliverables and the result of the project is the world's first SDN network solution that greatly improves the network performance increasing the reliability of the energy sector communications but also greatly increases the cybersecurity of the Ethernet network deployed on the Energy systems.

After the field test is complete, all three organizations will contribute to a Best Practices Guide.
Task 3.0 Authorship of best practice guide explaining how to test, deploy, and manage the technology for the long term.

These are released as the manual and datasheets

D. DELIVERABLES – All completed and submitted with successful results

1) Revised project management plan
2) Topical report on Open source code/technology that the project will use – this report will detail which protocols and technology were selected to accomplish the functional requirements and how the team designed to be interoperable with other managed switches or network management software on the market.
3) Topical report on system functionality and specifications – will describe what the commercial product will do and how the product is envisioned to be used on the system level
4) Topical report on commercial product development and release – this report will detail the completed stages of development and explain any engineering tradeoffs that happen throughout the development that made the team deviate from original functionality plan. This report will also detail the lessons learned in integration of open source code to accomplish the functionality in an interoperable way.
5) Topical report on the test plan – this report will detail the tests to be run on the product at CenterPoint facilities
6) Topical report on test results – this report will detail the results of the functional and environmental test run on the product
7) Topical report on administrative procedures to operate the network management software

8) Best practice guide report – this will explain how to test, deploy, and manage the technology for the long term.

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

Milestone Description	Estimated Completion	Actual Completion
Complete revision of the project management plan.	10/2010	10/2010
Project Start Date	*10/2010*	10/2010
Complete identification of all functional requirements for a managed switch with deep packet inspection	3/2011	3/2011
Bi-annual Review #1	*3/2011*	3/2011
Complete review of open source technology for functional solutions and identification of interoperable opportunities for configuration and logging	6/2011	6/2011
Topical report on open source technology to be employed on the product.	6/2011	6/2011
Complete hardware specifications that can support the required communication speed and uphold control system reliability needs	7/2011	7/2011
Complete authorship of use cases.	8/2011	8/2011
Bi-annual Review #2	*9/2011*	9/2011
Complete authorship of the detailed technical specifications of the hardware and firmware for the commercial product	9/2011	9/2011
Provide Topical report on system functionality and specifications describing the commercial product and its use on the system level.	9/2011	12/2011
Complete the design of the user interface of the commercial product.	12/2011	1/2012
Gate 1 Exit - Go/No-Go	**1/2012**	1/2012

Milestone Description	Estimated Completion	Actual Completion
Decision Point		
Bi-annual Review #3	*3/2012*	7/2012
Hardware circuit design and review complete	8/2012	10/2013
Bi-annual Review #4	*9/2012*	7/2012
Hardware prototype environmental testing complete.	12/2012	4/2014
Bi-annual Review #5	*3/2013*	DistribuTech
Hardware prototype 2 complete	4/2015	4/2015
Bi-annual Review #6	6/2015	3/2015
Firmware code written and unit tested	4/2016	6/2016
Complete the development of the commercial product.	6/2016	7/2016
Gate 2 Exit - Go/No-Go Decision Point	**3/2016**	**7/2016**
Topical report on the commercial product development and release	6/2016	9/2016
PHASE 2: Testing & Demonstration		
Topical report on the test plan detailing tests to be run at end user.	1/2016	9/2015
Complete prototype lab testing at end user facilities to make sure the team is on track to accomplish the technical and business requirements.	4/2016	3/2016
Completed execution of field demonstration of the commercial product at the end user.	6/2016	3/2016
Topical report on test results	6/2016	3/2016
Project close-out	**6/2016**	**9/2016**

Project Activities

The first key to success is to capture the right idea for the right problem use case. The Watchdog Project built on the successful team from the Hallmark Project which was originally funded under DE-PS26-07NT43119-00. The Hallmark Project secured serial communications

and the team identified the value of switched packet networks beyond the serial communications so our attention moved to identify how we could establish secure communications on those networks. Many of the Energy sector protocols are layer 2 protocols so we focused on the local area network first. Network access control and policy based enforcement and baselining were identified at the top of the requirements. This lead the team to need deeper packet inspection beyond layer 2.

The second key to success is to complete a solid plan. The team used the same project management plan that was successful for the Hallmark Project, we all knew the process and were successful the first time. This turned out to be a great idea as the project management plan for the Watchdog project allowed us to react to challenges and research results to adapt and to complete a very challenging project with 100% success. All team members understood their role and responsabilities, SEL to do the commercial development and release of the technology, CenterPoint and Ameren to provide technical and business requirements and pass fail criteria for the technology and for PNNL to help with security design and testing throughout the project.

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

- Research, develop, test, and commercialize a multi layer inspection switch to provide network access control.
- End user 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 Watchdog project addressed *Topic Area of Interest 5: Secure Communications*, by protecting the control system local area network itself and the communications coming from and going to the electronic devices on the local network. Local area networks usually are not routed and have little or no filtering capabilities. Combine this with the fact control system protocols are designed with inherent trust the control system owners have very little choice on how to protect communications on the local network. The Watchdog project reduces security risks in electric sector control system local area networks (LANs) by providing:

- Network access control (NAC)
- Multi-Layer firewall (physical through transport layer)
- Whitelisted protocols and message types allowing identification and containment of malware spreading across the network or unauthorized communications
- Configurable flow and path traffic engineering

This project improves operations and mitigate local area network risks by providing important tools to improve the ability to securely manage the control system LAN and the equipment connected to this LAN. These tools include:

- Providing multi-layer filtering to all traffic on the network at each hop.
- Automating LAN resiliency through identification and reaction to unauthorized traffic providing containment of malicious traffic
- Logging and reporting events and actions occurring at all layers of the network
- Replicating switch configurations for a secure and trusted method for contingency planning or network appliance backup

This project supplies the Energy sector with control system hardened and tested equipment that will provide network access control and network defense solutions. Projects like the DOE funded Lemnos Project have provided solutions for perimeter defense for control systems. The Watchdog project in contrast provides the next layer of defense at the local network layer which moves one step closer to the end device. The commercial product that was produced under

this project is being integrated into both existing and new control system networks enabling the Energy infrastructure to improve uniformly without limitations due to protocols or vendor specific equipment requirements.

This project fulfills important milestones in both the DOE Roadmap to Secure the Energy Sector and the NERC CIP standards. The Watchdog project provides “widespread implementation of methods for secure communication in a scalable and cost-effective to deploy” which is a milestone identified in the DOE Roadmap. The Watchdog project also provides solutions for CIP-005 and CIP-007 by providing strong access control to the local area network and allows the asset owner to control what protocols, messages or commands, and what devices can communicate to other devices in a network. Ultimately this provides the granular change control tools needed to lock down and monitor the field control system networks to make sure they continue to stay in a known good state.

Outcome and Benefits: This project produced the world’s first industrial focused SDN switch commercially available. This solution enables system operators to traffic engineer and protect the local area networks to stronger network access control then has ever been available. 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 Watchdog 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.

Watchdog Project team activities

The team pulled together well and the experience from each of the stakeholders was perfectly balanced. Our first activity was to capture the use cases and industry requirements. This was lead by CenterPoint and 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.

The project team started down the path to develop a traditional network switch with RSTP and have deep packet inspection capabilities. The first prototype design went thorugh the heat exchange calculations and the design quickly failed the exercise. There were not processors fast enough to keep up with full backplane bandwidth and do deep packet inspection for every port on the switch and comply to the Energy sector environmental conditions. This was the cause of the first project schedule adjustment as the team had to go back to the drawing board and find a new way to accomplish the same goals without deep packet inspection for traditional

networking. The team then identified SDN, this was a new and promising network architecture to abstract the control plane from the data plane and be Ethernet packet layer independent. The team had concerns as it was brand new in 2011 so the team proceeded with caution. The Linux Foundation backed the SDN technology and the industry started to all get behind this new design so we proceeded. The second prototype showed we could design hardware to support SDN and the environmental conditions. The team then worked to apply OpenFlow to the proactive traffic engineering we needed in the critical infrastructure industries which is much different then the data centers and carriers that SDN was beig deployed. The research proved it could be successful and performance and cybersecurity will improve greatly. This lead to the development and commercial release of the SEL-2740S the world's first industrial SDN switch.

SEL-2740S Software-Defined Network (SDN) Switch

Traffic-Engineered Ethernet Communication for Substation and Plant Networks

Major Features and Benefits

The SEL-2740S SDN Switch is a 20-port switch designed for the harsh environments common to critical infrastructure industries. The SEL-2740S is a deny-by-default network switch that enables full control of Ethernet traffic engineering. Traffic engineering provides you the ability to configure each communications flow path, configure flow match filters for approved forwarding, and pre-engineer failover conditions to design fault-tolerant networks. The result is greater performance, improved reliability, and more deterministic packet delivery.

- **Reliability.** Provides a robust design built and tested to function in harsh environments, meeting IEEE 1613 and IEC 61850-3 standards. Hot-swappable, dual power supplies provide connectivity to primary and backup power sources.
- **Fast Failover.** Allows healing in microseconds with proactive traffic engineering for fault conditions.
- **Modularity.** Provides six hot-swappable modular interface slots and two power supply module slots.
- **Cybersecurity.** Supports deny-by-default network access control and secure management of communication with OpenFlow 1.3 through Transport Layer Security (TLS) and the detailed central monitoring capability of the SEL-5056.
- **Flexible Group and Action Bucket Support.** Supports 256 groups and 30 action buckets per group, enabling flexible network design and traffic engineering.

The SEL-2740S requires one alarm contact and flow coprocessor module, and it provides the installation option of as many as five Ethernet interface modules and two power supply modules.

- **Redundancy.** Provides strong, central management of all traffic flow circuits and backup circuits. Also provides operational statistics from the flow controller.
- **Ease of Use.** Supports quick commissioning and all network configuration programming through the SEL-5056 SDN Flow Controller.
- **SDN Management.** Supports OpenFlow® 1.3.
- **Low-Latency Flow Setup.** Allows quick establishment of flows through the use of low-latency controller and table updates.
- **Low-Latency Forwarding.** Provides store-forward, low-latency forwarding.
- **Large Flow Table Size.** Supports small and large networks with a 4,096 flow entry capacity.
- **Packet Buffer Memory.** Supports 87 packets at maximum transmission unit (MTU).
- **Switching Capacity.** Supports a 5.6 Gbps packet data rate and full duplex, nonblocking design.
- **Forwarding Match Filters.** Provides control of all network forwarding through each hop by allowing configuration of match attributes for each flow on Layer 1, 2, 3, or 4 fields.
- **Quality of Service (QoS).** Provides traffic priority management through four 8:4:2:1 weighted round robin (WRR) priority queues, directly selectable or through priority code point (PCP) values.
- **Network Time Protocol (NTP) Time Synchronization.** Allows time synchronization through NTP and operation as an NTP client to time-align events and user activity across the system.
- **X.509 Certificate.** Supports secure communication between the switch and the flow controller, and manages keys through certificates.

PNNL performed threat modeling for the design and fed the results to SEL for inclusion into the project before commercialization. After the product was developed PNNL also performed negative testing and fed the results back to SEL for improvements. PNNL advised SEL during the product development.

Ameren joined the effort half way through the project as they joined the SDN Project and when the Watchdog and SDN project joined forces they participated in the Watchdog guidance and end user testing. CenterPoint was challenged to stay connected and the team continued with the participants that could provide engagement whenever they could. The good news is that a variety of end users participated so the team was never without end user guidance at any point in the project. The end user testing was performed at the Technology Application Center (TAC) at Ameren. This testing went so well that we finished a day early. The team had produced a test plan from the use cases and technical and business requirements the end user provided, all tests were completed with 100% success.

Products Developed

The Watchdog Project Team completed the following products

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

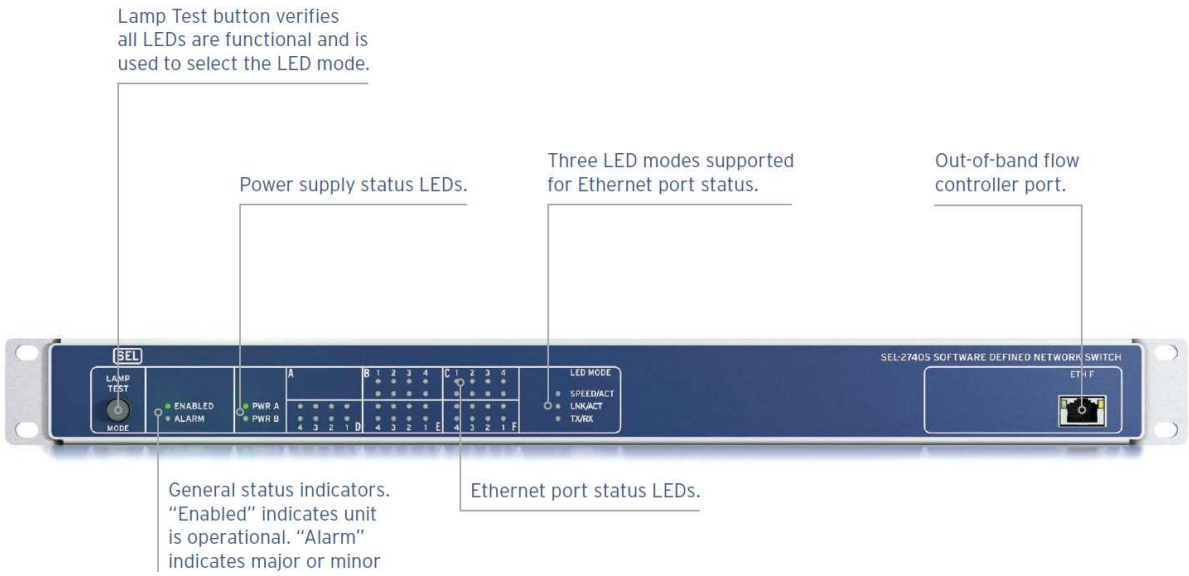
Software-Defined Networking Addresses Control System Requirements

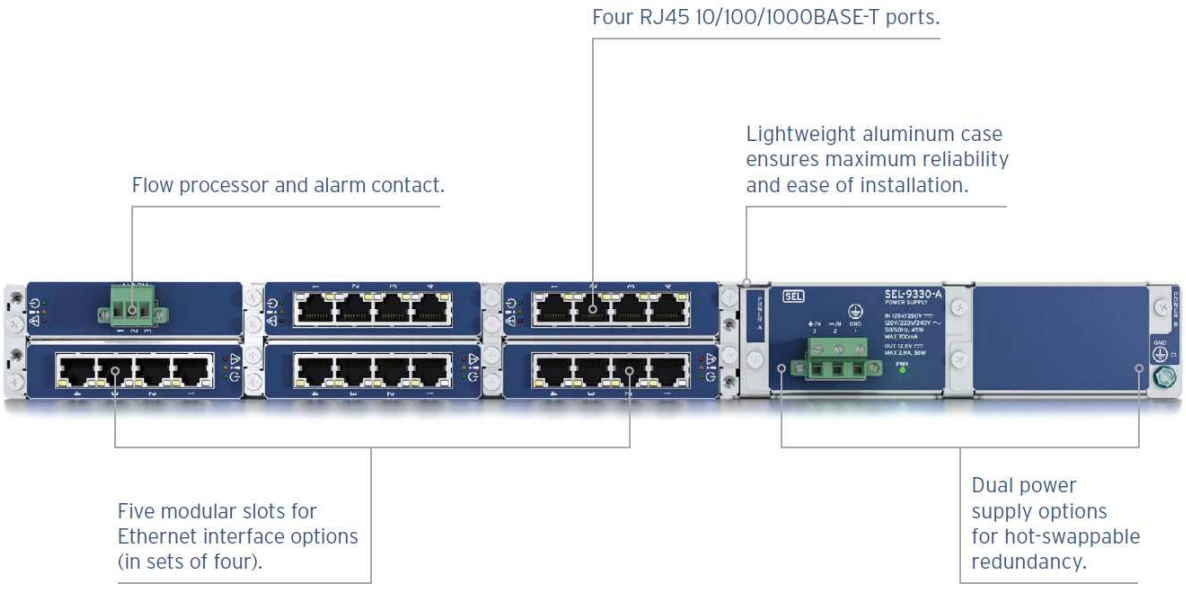
Rakesh Bobba, *University of Illinois at Urbana-Champaign*
Donald R. Borries, Rod Hilburn, and Joyce Sanders, *Ameren Illinois*
Mark Hadley, *Pacific Northwest National Laboratory*
Rhett Smith, *Schweitzer Engineering Laboratories, Inc.*

***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 running on a single physical communications channel. However, this still leaves gaps in the capabilities that the engineers designing this critical infrastructure desire that corporate networking technology does not provide. Examples of these gaps include preconfigured primary and failover forwarding paths from end to end, calculated and repeatable latency resulting in managed determinism, and system-wide detailed visualization and monitoring capability, as well as deny-by-default security at all layers of the communications system.

In searching for answers on addressing these gaps, the

2) Commercially released SEL-2740S Software Defined Network Switch
www.selinc.com/SEL-2740S





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-2740S

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

5) One patent were filed under this project and was awarded. The patent number is 9,300,591 for the US Patent office. SEL submitted a report to DOE in compliance with 10 CFR 600.325

Computer Modeling Involved

No computer modeling was produced in the SDN Project.

Conclusion

The Watchdog Project team completed all tasks in the SOPO in the originally approved form and identified some additional work within scope to complete and after getting the SOPO edited completed that work as well successfully without increasing the budget. The team managed the project with the approved Project Management Plan and did not alter that plan over the life of the project. The budget did not change the federal funds after the originally approved budget in October 2010 but the project did take six years instead of three years. The extra time and effort expenses were covered by SEL and contributed as cost share.

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.