U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Software Defined Networks for Energy Delivery Systems (SDN4EDS)

Pacific Northwest National Laboratory (PNNL)

Scott R. Mix, CISSP, PM / Mark Hadley, PI

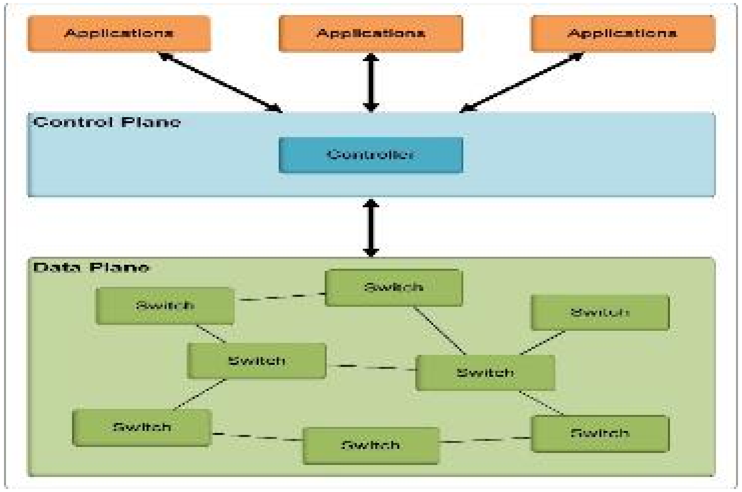
Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Summary: SDN4EDS

Objective

- Increase the adoption of SDN technologies and improve security for LANs and WANs, by decreasing the attack surface and increasing situational awareness, engaging the SDN vendor community to develop trust models, and testing interoperability for software and hardware components.



Schedule

- October 2017 – September 2020
- Phase 1 – Develop & Deploy Blueprint Architecture
- Phase 2 – Develop & Test Cyber Analytics and Trust Models
- Phase 3 - Develop EDS Protocol Behavior Solution

Total Value of Award:	$ 2,500,000
Funds Expended to Date:	11.38%
Performer:	Pacific Northwest National Laboratory
Partners:	AECOM, CAISO, Dispersive, Juniper, NREL, SCE, SEL, SNL,

Advancing the State of the Art (SOA)

- SDN is a mature technology in IT environments, and is an emerging technology in OT environments
- OT practitioners may be unfamiliar with SDN technology
- Standard IT SDN technology is not completely applicable in an OT environment
- SDN4EDS demonstrates how SDN can be implemented at scale in an OT environment
- SDN has the potential of significantly increasing resilience and security of OT networks

Challenges to Success

Contracts not in place

- Ongoing discussion with remaining partners
- Alternative partners and solutions being evaluated

Numerous partners expressed sensitivity to disclosing technical details to competitors on the project

- Mitigated by posting messages to not disclose any business or technically sensitive detail in group meetings

Multi-vendor environment

- It is unlikely that one partner will have all the solutions being sought by the project
- Multi-vendor environments are inherently more difficult to manage
- Mitigated by using open-source solutions adopted by multiple vendors
- Mitigated by using industry end-user partners as an advisory board with broad skill set and active engagement in the industry to stay abreast of developments

Progress to Date

Major Accomplishments

- The SDN Blueprint Reference Architecture document developed and updated in each project
    - Three versions (February, May, September, 2018) of *Software Defined Networking for Energy Delivery Systems (SDN4EDS) - An Architectural Blueprint by* Mix S.R., M.D. Hadley, and S.V. Singh
- Table-top Red Team assessment of initial reference architecture completed
- Each version of the Blueprint Reference Architecture document expands technical and background information for final product to industry
- A test lab is being set up at PNNL to perform additional experimentation and red-team efforts

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Intellectual Property Management Plan developed and approved by partners
- Technology Transfer Plan work this next year
- Blueprint Reference Architecture document (major project deliverable)
  - Contains full information on reference architecture implemented and tested in lab
  - Contains industry use cases and migration strategies
  - Will allow industry to try a tested SDN environment in their own labs
- Developing technical papers discussing project and technology

Next Steps for this Project

Approach for the next year or to the end of project

- Finish lab setup
- Expand lab to include SD-WAN technology
- Perform red-team assessments of lab environment
- Develop performance and security analytics providing situational awareness to EDS network operators
- Develop protocol-aware flow rules to implement firewall/IDS functions within the core network
- Continue updating the Blueprint Reference Architecture document