SEL SCHWEITZER ENGINEERING LABORATORIES

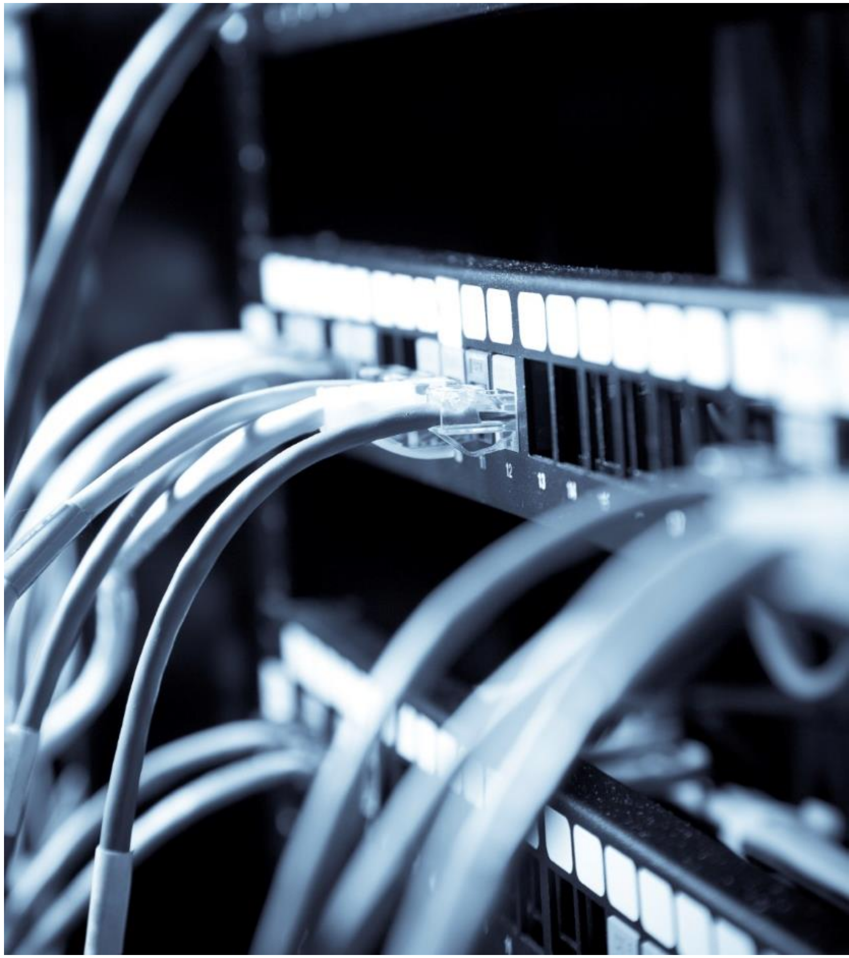
Watchdog & SDN Projects

Cybersecurity for Energy Delivery Systems Peer Review

Dec 7-9, 2016

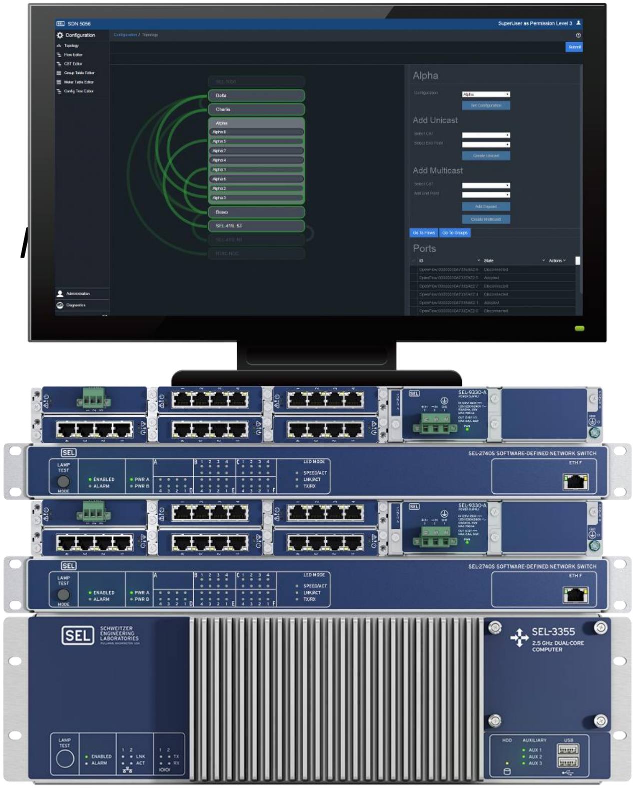
CEDS Roadmap

- **Watchdog Project**
  - Topic Area 5: Secure Communications
    - Network access control
    - Multilayer packet inspection
    - Identify and contain unauthorized communications
    - Whitelist deny-by-default
- **SDN Project**
  - Topic Area 2: Sustain critical operations while responding to cyber-intrusion
    - Greater situational awareness
    - Disruptionless change control
    - Scalable and cost effective IDS/IPS solutions



Summary: Watchdog & SDN Projects Completed and Commercially Released!

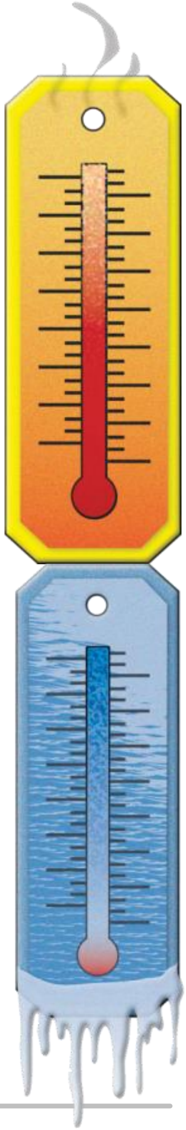
- **Objective**
  - All networks become deny-by-default whitelisted proactive traffic engineered
  - Economical solution for multilayer packet inspection providing LAN traffic filtering
- **Technical Approach**
  - Collect industry needs both technical and business
  - Research best solutions – SDN
  - Design, develop, test, release
- **World's First OT SDN Solution!!**
  - https://selinc.com/products/2740s/
  - https://selinc.com/products/5056/


SDN 5056
Configuration
Alpha
Add Unicast
Add Multicast
Ports
SEL
SEL-2740S SOFTWARE-DEFINED NETWORK SWITCH
SEL-9330-A
SCHWEITZER ENGINEERING LABORATORIES
SEL-3355
2.5 GHz DUAL-CORE COMPUTER

- **Performers:** CenterPoint, PNNL, Ameren, UIUC, Oregon St, SEL

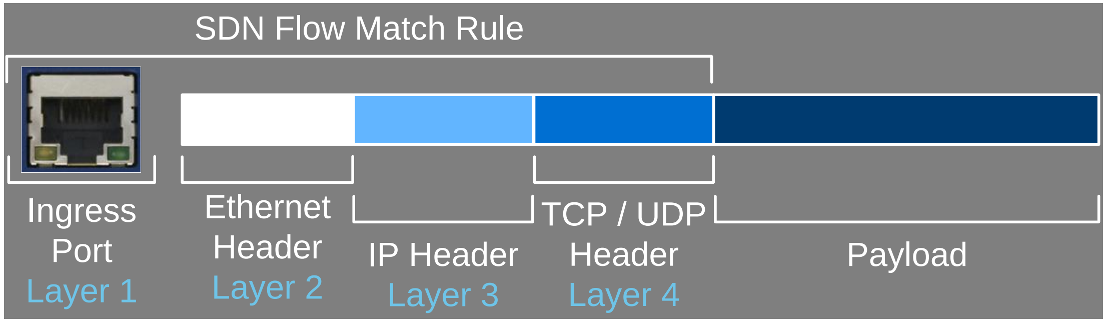
Technical Approach and Feasibility

- **Normal Approach**
  - Watch and react to bad traffic
  - Signature or configuration updates
  - Single point in communication path
- **Watchdog & SDN Approach**
  - Only allow approved traffic proactive flow programming
  - Only allow approved clients multilayer match criteria
  - Integrate in appliance already needed, SDN switch
  - Changes only needed when protocols or devices change



Advancing the State of the Art

- **Better situational awareness**
  - OpenFlow counters
  - Packet and path-level control
- **Stronger cybersecurity**
  - Multilayer packet inspection at each hop
  - Removal of vulnerable control plane
  - Secure the control plane through TLS
  - Simplified IDS/IPS architectures and loads through table miss entry
- **Greater performance**
  - Fault heal times <100uS
  - Maximize switch efficiency
  - Disruptionless scalability



Technical Achievements

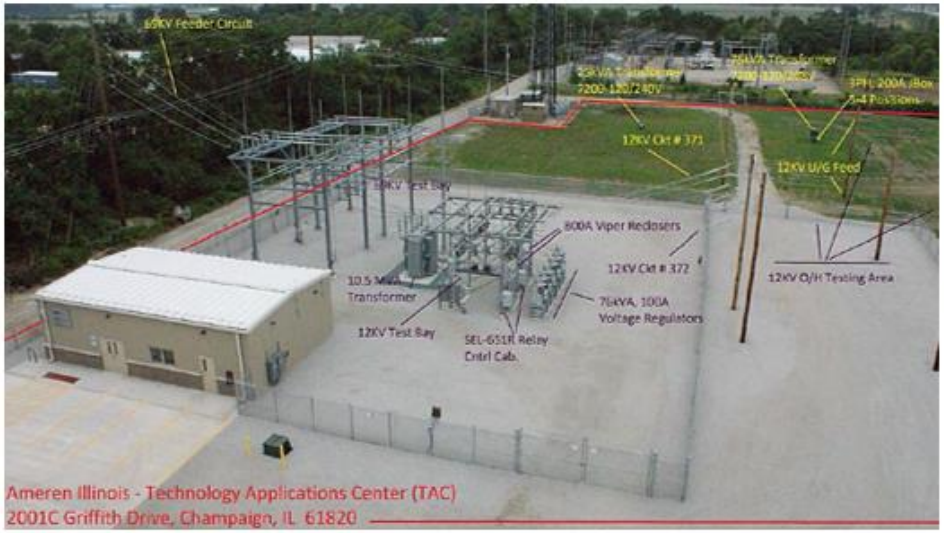
- **Developed and commercially released the SEL-2740S**
  - World's first OT SDN switch
- **Developed and commercially released the SEL-5056**
  - World's first OT SDN flow controller
- **Designed to open source standards maximizing interoperability and scalability**

OpenFlow™

SDN

Validated Technology

- **Supporting the technical and business needs**
- **Improving reliability at the same time as cybersecurity**



The SDN project team (from left to right): Tamer Rousan, Ameren; Faisal Hasan, University of Illinois; Don Borries, Ameren; Rhett Smith and Robert Meine, SEL; and Abhilash Raj, Oregon State

SEL completes successful onsite testing of first substation software-defined network

Ameren onsite validation exceeds expectations

Conclusions: Watchdog & SDN Projects

- Met every task and deliverable in project objectives
- Resulted in world's first OT SDN solution
- Greatly improves cybersecurity, reliability, performance, and usability of control system Ethernet networks
- Redefines what is possible on Ethernet networks
- Being deployed now at many critical infrastructure organizations ranging from DoD to Industrial to Electric to O&G

Next Steps

Poster Session for Details

Chess Master Project

SEL

Sempra Energy for every day life.®

Ameren

VERACITY Industrial Network Security