**Summary: Watchdog Project**

- **Objective**
  - Managed switch with application layer firewall and network access control
  - Economical alternative to IDS/IPS and provide LAN traffic filtering

- **Technical Approach**
  - R&D 24-port managed switch with whitelist and blacklist DPI and NAC
  - Develop hardware, SEL-2730S
  - Research methods for ease of use
  - Design ways to administrate, monitor and respond
  - Validation testing at PNNL
  - End user testing at CenterPoint Energy

- **Schedule**
  - Commercial release May 2014
  - Field trial completion July 2014

- **Performers: CenterPoint, PNNL, SEL Energy**
Technical Approach and Feasibility

- **Normal Approach**
  - Watch and react to bad traffic
  - Quick signature or configuration updates
  - Single chock point in communication path

- **Watchdog Approach**
  - Only allow approved traffic (DPI) than blacklist specifics
  - Only allow approved clients (NAC)
  - Integrate in appliance already needed
  - Changes only needed when protocols or devices change
  - Provide alternative to firmware upgrades
  - IEEE1613 compliant
Technical Approach and Feasibility
Challenges to Success

- **Local Area Network Protection**
  - Deep packet inspection
  - Network access control
  - Detailed logging
- **Speed and ease of use**
  - DPI must happen in HW
  - Regular expression vs frags or split data
  - Configuration
  - Diagnostics
- **Change control**
  - Whitelist approved traffic
  - Policy server infrastructure
- **Threat assessment**
Technical Approach and Feasibility
Technical Achievements to Date

- Hardware design and calculations complete
  - Switch fabric in hardware
  - DPI in hardware, regular expression
  - Processor for NAC, logging, admin

- Hardware prototypes being built
  - FPGA next generation
    - Altera Arria V
  - Form factor complete

- Configuration design
  - PNNL user interface group
  - PNNL provided evaluation on current trends
Collaboration/Technology Transfer

• **Plans to gain industry input**
  – Watchdog team building on success of Hallmark with end user (CenterPoint), lab (PNNL), and manufacturer (SEL)
  – SEL is working with additional utilities to discuss design trade offs and system requirements

• **Watchdog team advantages**
  – PNNL and SEL geographically close
  – CenterPoint automation expertise providing technical and procedural requirements
  – Principle investigators are more experienced with PDLC and cross company cooperation
Progress To Date

- **Hardware design almost complete, Q4 this year**
  - IEEE1613 class 2
  - 1U rack mount
  - Four 1G, four SFP, fifteen 10/100M ports
- **NAC technology selected to be 802.1X**
- **Hardware acceleration required and planned for**
- **Developed control system switch fabric foundation**
  - VLAN tagging
  - MAC filtering
  - Central monitoring SNMP and Syslog
Next Steps

• **Approach for the next year or end of project**
  – Commercially release SEL-2730S
  – Field evaluations
  – Best practice guide on test, deploy, and manage

• **Project results that may form the basis of future control systems security work or link to other programs/organizations**
  – DPI efforts at Telcordia and TCIPG
  – NAC infrastructure into trust management projects
Conclusions: Watchdog Project

• Moving one step closer to end device
• Addressing major project risks early
• Providing bad traffic containment
• Considering trust management needs first
• Advancing educational requirements and training
• Monitoring and design to NERC CIPv5 requirements for IDS to make sure this technology will fulfill needs