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

Survivable Industrial Control Systems
Sandia National Laboratories (SNL)

Adrian R Chavez

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

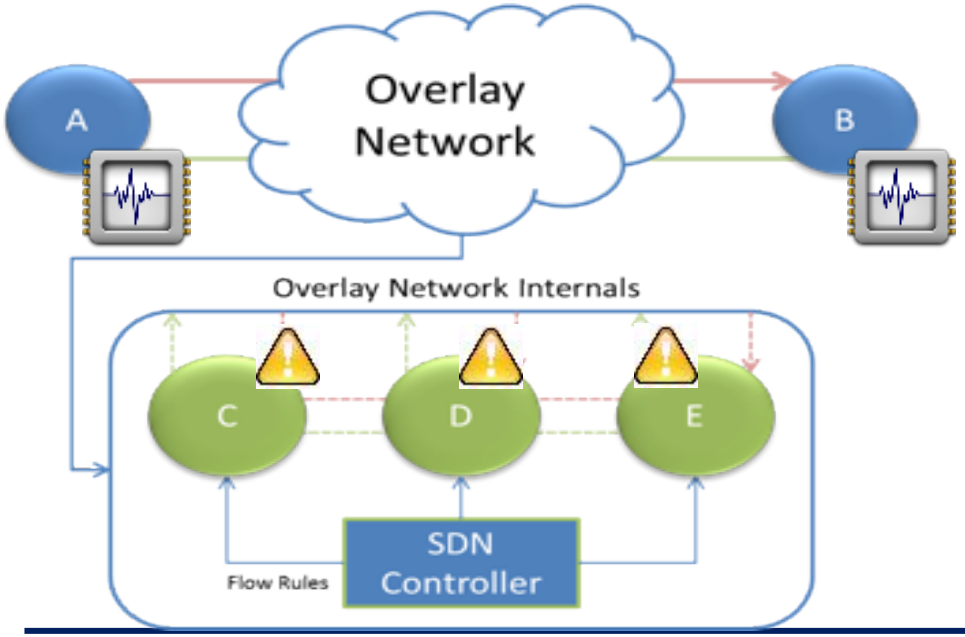
Summary: Survivable Industrial Control Systems

Objective

- Proactively detect and appropriately respond to threats automatically by advancing and building upon ADDSec and Cyber Physical Modeling for Situational Awareness (CYMSA) projects.

Schedule

- 11/1/18-10/31/21
- Kickoff meeting 5/10/18; Contracts complete 9/25/18
- Cyber/physical monitoring included in ADDSec, behavior based analysis on SDN traffic/flows, and SDN enforced responses



Total Value of Award:	**$2.5M**
Funds Expended to Date:	**0.6%**
Performer:	**Sandia National Laboratories**
Partners:	**Chevron, Grimm, GTRI, PNNL, SEL, and Ft. Belvoir NVESD**

Advancing the State of the Art (SOA)

- Detection and response continue to be reactive to current threats
- Practical guidelines for MTD parameter settings are limited. The conditions for correct cost-effective MTD use are poorly understood
- Cyber/physical security systems are separate from existing OT infrastructure
- Behavioral based analysis of SDN traffic and flows needed
- SDN controller, in reactive flow installation mode, is a single point of failure
- DoD software deployments must go through Certification of Networthiness process
- Modeling and simulation must meet real-time constraints of OT environments

Advancing the State of the Art (SOA)

- **Combine ADDSec and CYMSA to enhance automatic detection and response capabilities for increased resiliency**
- **Correlate events from SDN flows and host based events**
- **Apply DoD Certification of Networthiness process to ADDSec technologies**
- **Distribute SDN controller**
  - Reduce load
  - Eliminate single points of failure
  - Establish fault-tolerant systems
- **Broadly apply ADDSec and CYMSA to electric and Oil & Natural Gas (ONG) sectors**
- **Optimize moving target defense strategies through game-theoretic approaches**
- **Build accurate real-time models of partner sites to evaluate security of active OT environments**

Progress to Date

Major Accomplishments

- Kickoff meeting (May 10, 2018)
- Contracts for all partners completed (9/25/18)
- Project start with all partners (11/12/18)
- Distribute SDN controller (6/12/19)
- Correlate SDN traffic (10/12/19)
- Integrate ADDSec and CYMSA technologies (11/12/19)
- Independent 3rd party red team assessment (2/12/20)
- Integrate ADDSec and CYMSA into partner site (5/12/21)
- Capture performance metrics of partner site (8/12/21)
- Final report (11/11/21))

Challenges to Success

Build an accurate model of partner site

- Work closely with partners
- Leverage existing CYMSA real-time modeling environment

Combine ADDSec and CYMSA within partner site

- Include CYMSA alerts as detection module into ADDSec framework

Distribute SDN controller within partner site

- Leverage SDN clustering
- Work closely with partners

Complete Certification of Networthiness process for DoD-wide deployment

- Work closely with partners who have already completed the process

Collaboration/Technology Transfer

Continue working with partners and expanding detection response framework

- Targeting both vendors and asset owners
- Working with Chevron, Ft. Belvoir, and SEL to guide/drive our R&D towards commercialization
- Independent red team assessment
- Demonstration and testing at completion of project at partner site
- Compatible with OpenFlow 1.3
  - Existing open source and commercial SDN switches compatible with ADDSec
- Patent issued on ADDSec technology