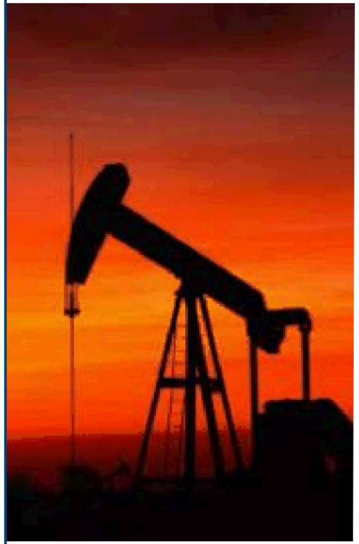
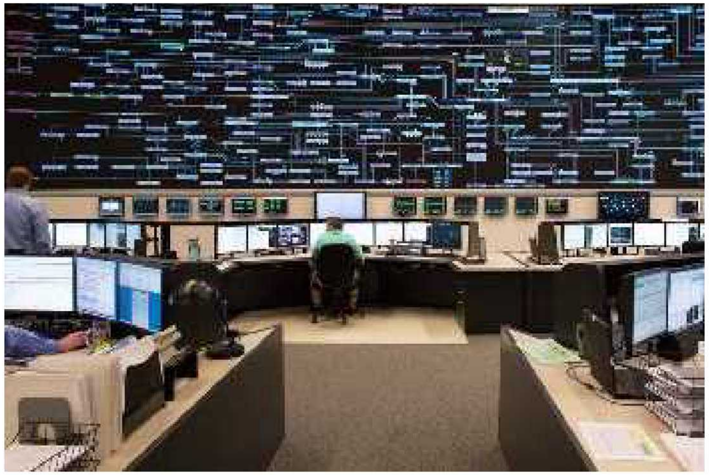
U.S. DEPARTMENT OF
ENERGY

Office of
Cybersecurity, Energy
Security, and
Emergency Response





SAND2018-12268PE

Adrian R Chavez

Sandia National Laboratories

Artificial Diversity and Defense Security (ADDSec)

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.

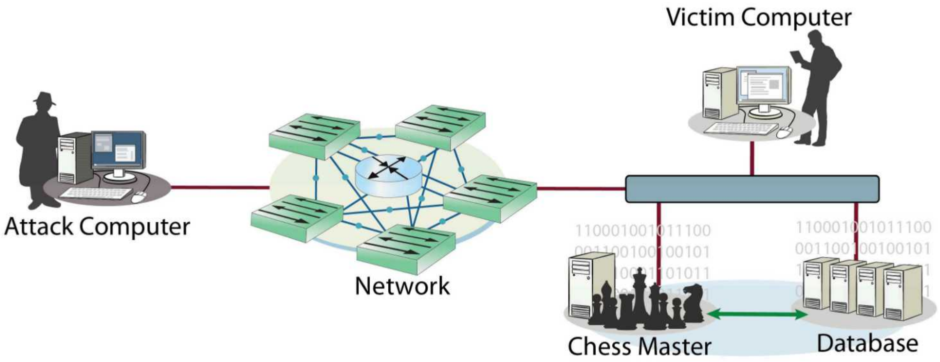
Summary: Artificial Diversity and Defense Security (ADDSec)

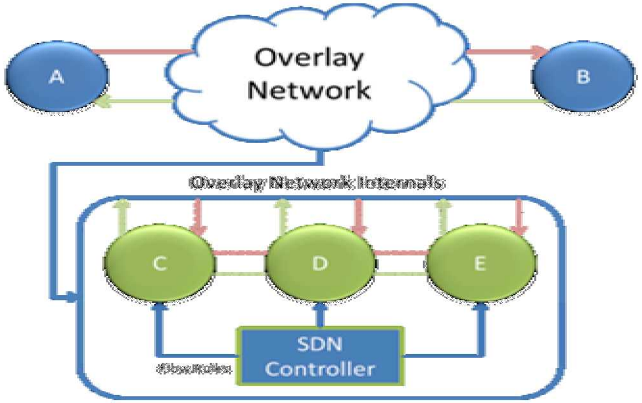
Objective

- Build a framework to proactively detect and appropriately respond to threats while meeting the constraints of an ICS environment. Detection is based on machine learning algorithms and responses are focused on moving target defenses.

Schedule

- 9/22/2015- Present
- Laboratory testing 1/20/17; Ft. Belvoir NVESD demonstration 7/27/18; Report documenting technology and demonstration 4/30/18
- Machine learning algorithms and moving target defense solution leveraging Software Defined Networking compatible with devices using OpenFlow 1.3





Total Value of Award:	**$3M**
Funds Expended to Date:	**90%**
Performer:	**Sandia National Laboratories**
Partners:	**Chevron, Grimm, LLNL, SEL, and Ft. Belvoir NVESD**

Advancing the State of the Art (SOA)

- **Current defenses are reactive**
- **Moving target defense is an active area of research**
  - ASLR
  - IT Focused
  - Need to account for OT requirements and constraints
- **Machine learning and response are manual and requires operator intervention**
- **Software Defined Networking primarily used within IT sector**

Advancing the State of the Art (SOA)

- **We have developed a framework to automate detection and response to threats within OT environments**
  - Meet operational requirements (< 20 μs of delay)
- **Machine learning algorithms**
  - Ensemble set of ML algorithms that continuously evolve
- **Moving target defense strategies**
  - IP randomization
  - Port randomization
  - Communication path randomization
  - Application library randomization
- **Building off of Software Defined Networking**
  - Compatible with OpenFlow 1.3

Progress to Date

Major Accomplishments

- Developed detection modules (3/25/16)
- Developed response modules (9/2/16)
- Independent red team assessment (3/10/17)
- Laboratory testing (5/3/17)
- Partner site testing (2/1/18)
- Final report (4/30/18)

Challenges to Success

Evaluation of machine learning algorithms with representative datasets

- Initially work with publicly available datasets
- Capture host-based and network-based events for partner systems

Meet constraints and requirements of partner site OT environment

- Maintain connectivity between active communication sessions by building off of SDN
- Measure operational impacts of several randomization frequencies

Apply and combine ADDSec technologies within partner site

- Work with partners throughout entire project lifecycle

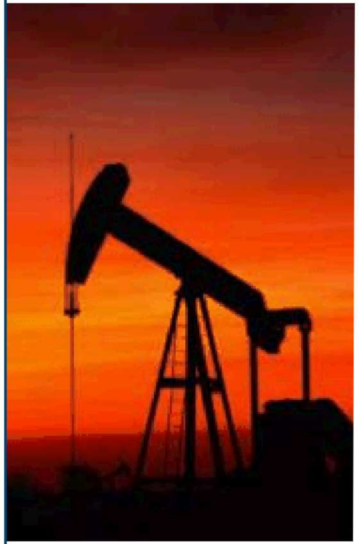
Collaboration/Technology Transfer

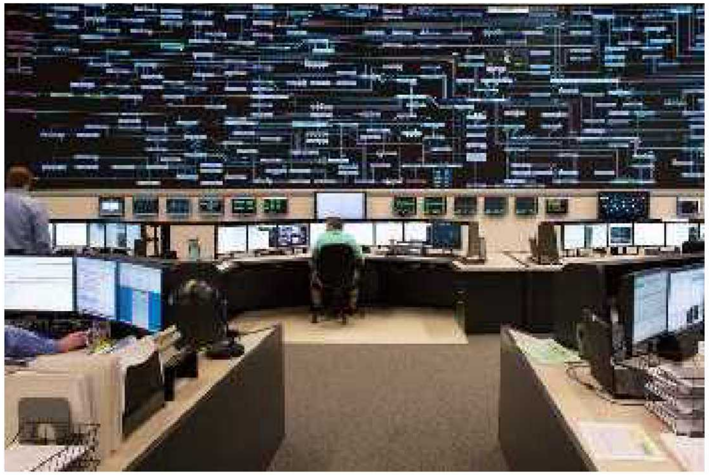
Continue working with partners and expanding detection response framework

- 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 complete
- Demonstration and testing complete at partner site
- Compatible with OpenFlow 1.3
  - Existing open source and commercial SDN switches compatible with ADDSec
- Patent issued on ADDSec technology

U.S. DEPARTMENT OF ENERGY

Office of Cybersecurity, Energy Security, and Emergency Response





Adrian R Chavez

Sandia National Laboratories

Survivable Industrial Control Systems

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.

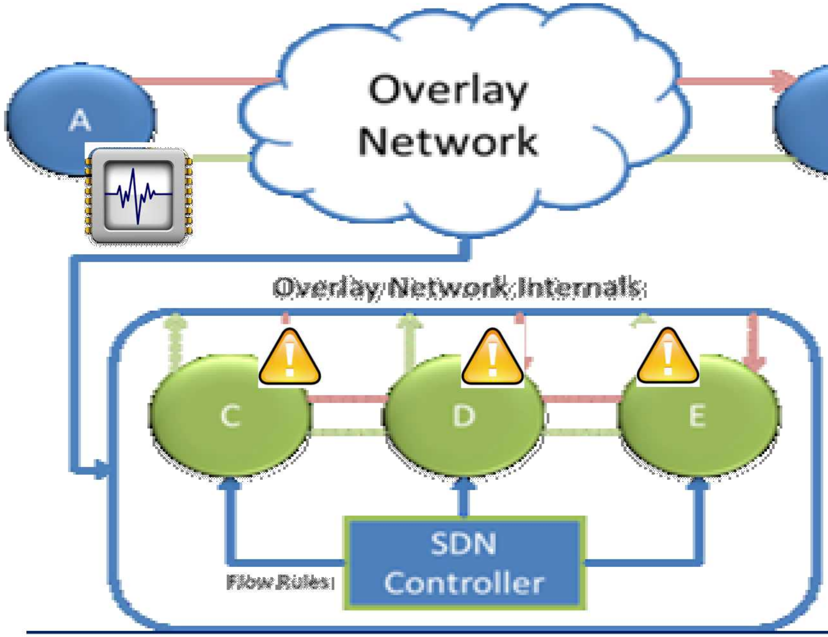
Summary: Survivable Industrial Control Systems

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 (2/12/19)
- 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

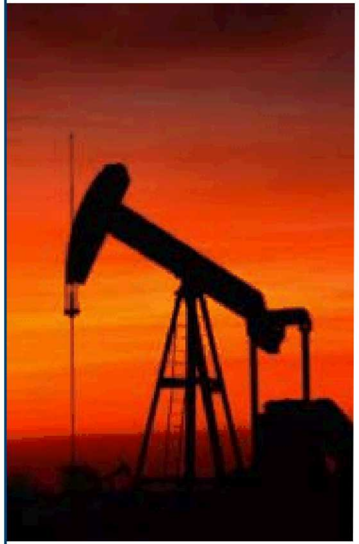
Collaboration/Technology Transfer

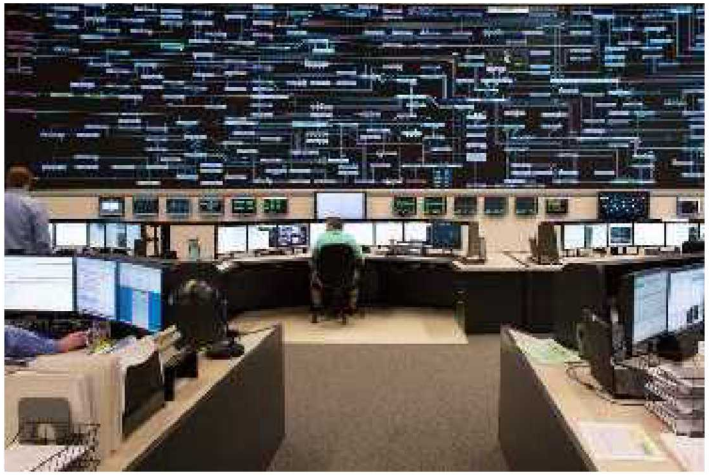
Continue working with partners and expanding detection response framework

- 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

U.S. DEPARTMENT OF
ENERGY

Office of
Cybersecurity, Energy
Security, and
Emergency Response





Adrian R Chavez

Sandia National Laboratories

Containerized Application Security for Industrial Control Systems

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.

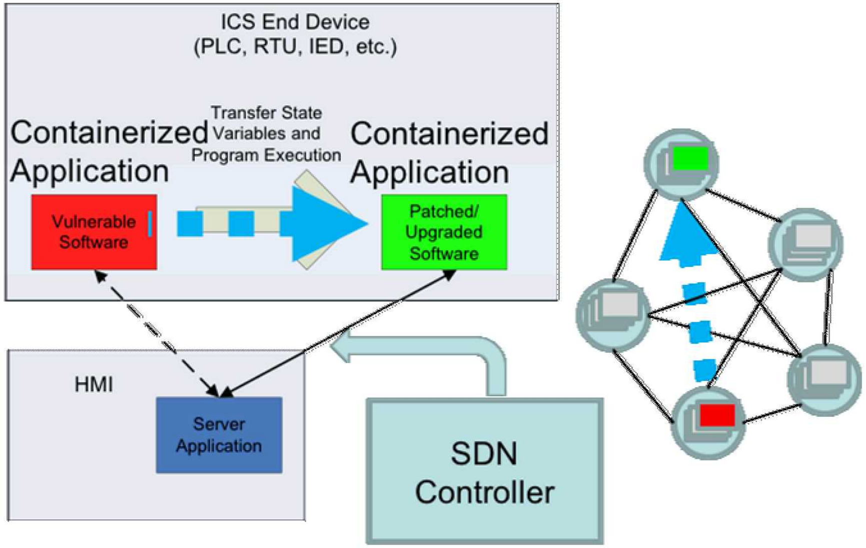
Summary: Containerized Application Security for Industrial Control Systems

Objective

- Increase the availability and resiliency of control systems by dynamically migrating, updating, and restoring applications during a cyber incident.

Schedule

- 5/10/18-5/9/21
- Kickoff meeting 5/10/18; Literature review 7/12/18; libmodbus containerized 10/4/18
- Updating software and creating a moving target defense at the application level in near real-time without interruptions in availability or operation.


ICS End Device
(PLC, RTU, IED, etc.)
Containerized Application
Transfer State Variables and Program Execution
Containerized Application
Vulnerable Software
Patched/ Upgraded Software
HMI
Server Application
SDN Controller

Total Value of Award:	**$2.5M**
Funds Expended to Date:	**4%**
Performer:	**Sandia National Laboratories**
Partners:	**Chevron, Grimm, PNNL, SEL, and Ft. Belvoir NVESD**

Advancing the State of the Art (SOA)

- Currently, interruptions in service are necessary to update/upgrade software
- BlackEnergy, Shamoon, and Stuxnet are examples of malware that targeted an application to propagate through a control system network
- Application containers used within IT environments but not within OT environments
- Virtual machines used within OT environments but heavyweight

Advancing the State of the Art (SOA)

- **We will leverage open source and open platform tools**
  - Docker, SoftPLC, libmodbus, and opendnp3
- **Containers isolate applications and help prevent lateral movements**
- **Docker containers checkpoint/restore in userspace**
  - Update/patch/upgrade software in near real-time
  - Increase resilience of OT environments
- **Moving target defense in live-migration creates uncertainty for adversary**

Progress to Date

Major Accomplishments

- Kickoff meeting (May 10, 2018)
  - Completed contracts for all partners
- Completed literature review on available container solutions (July 12, 2018)
  - Docker, Buildah, CoreOS Rocket, Linux Containers, Virtual Machines, Orchestration engines, …
- Developed use cases and scenarios (July 12, 2018)
  - Libmodbus, openDNP3, and SoftJace
  - SoftPLC
- Developed threat sceanario and con-ops (July 12, 2018)
- Libmodbus containerized (October 4, 2018)

Challenges to Success

Minimize downtime during upgrade/patching software in OT environments

- Leverage Docker CRIU capability
- Identify upgrade points with minimal state in software
- Checkpoint and transfer state of old software to upgraded software

Migrate application containers

- Leverage orchestration technologies (Kubernetes)
- Reroute traffic using SDN

Develop an interoperable solution

- Docker is portable across a number of operating systems
- Applications can be containerized with the aid of an executable or source code

Collaboration/Technology Transfer

Continue working with partners throughout R&D process

- 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 scheduled towards the end of year 2
  - Continuous input and communication throughout
- Demonstration and testing scheduled for project close out at partner site