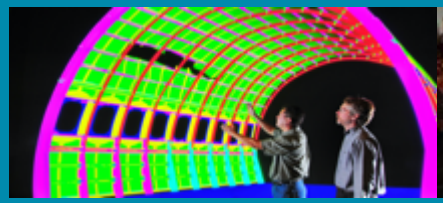
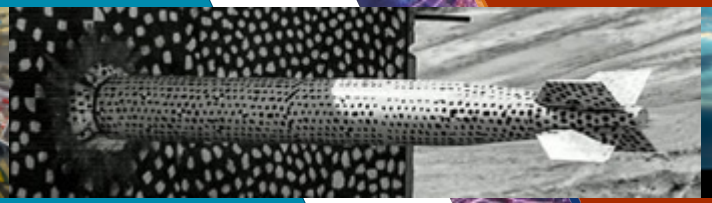
Sandia National Laboratories

Exceptional service in the national interest

SAND2020-11742PE








SANDIA NATIONAL LABORATORIES

MOSAICS – More Situational Awareness for Industrial Control Systems

Robert G. Cole, SNL

UPDATED OCTOBER 2020

U.S. DEPARTMENT OF ENERGY | NNSA

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.
SAND2019-11784 PE

Program (26 October 2020)

1130-1140: Introduction
Robert Cole

1140-1200: SNL Development Team
John Jacobellis

1200-1220: SNL SCEPTRE Development Team
Chris Abate

1220-1240: SNL Red Team
Tim Schulz

1240-1300: Questions

Non-Kinetic Threat

Timeline of Non-Kinetic Attacks on Critical Infrastructure

Chinese hackers target 23 U.S. gas pipeline companies collecting sensitive information

OASyS System files are collected

Havex watering hole-based ICS targeting

F-Secure notes 7 years of cyber espionage

Cyber attack directed against Ukrainian transmission operator

WannaCry
CrashOverride
Petya-NotPetya
Nuclear 17…

US Cert - Russian Targeting Energy & Critical Infrastructure

MOSAICS Technology Approach

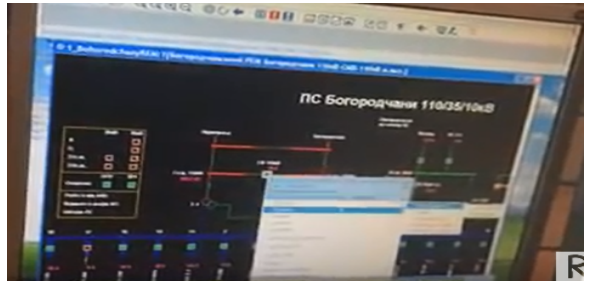
2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019

tuxnet
entified

Shamoon wiper destroys nearly 30,000 Saudi Aramco computers

Energetic bear collects data from energy companies in U.S. and Europe

Cyber attack directed against utilities in Ukraine



THREATS ARE REAL AND EXPANDING

FY18 Start

More Situational Awareness for Industrial Control Systems (MOSAICS) JCTD BLUF

Operational Objective:

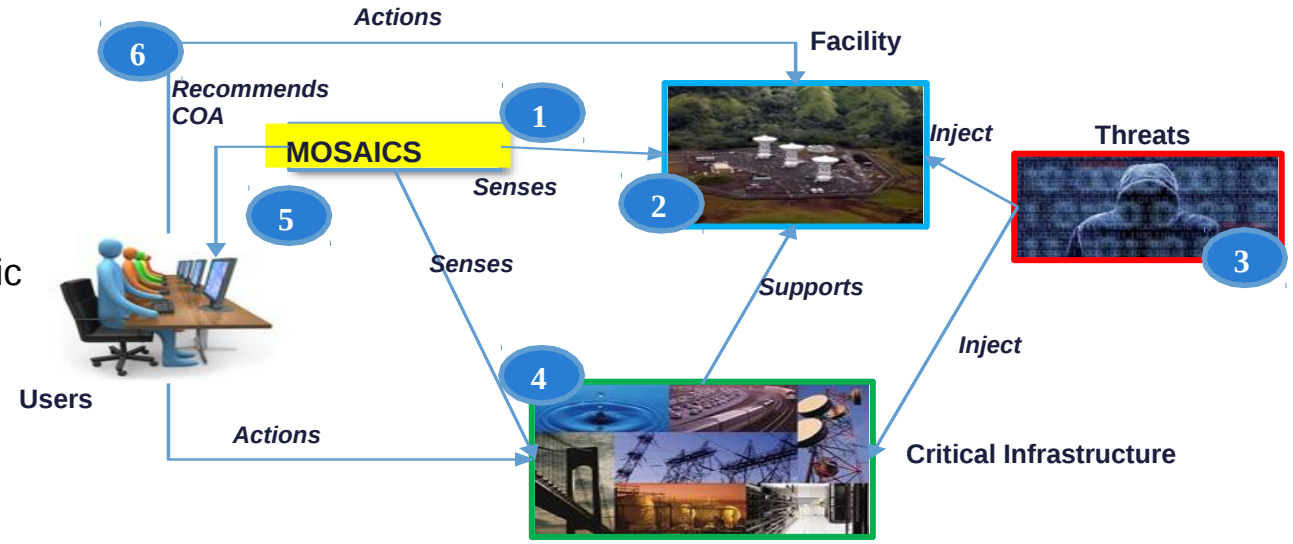
- The objective of MOSAICS is to create the initial operational defense of control systems of mission critical infrastructure from cyber attacks.
- Baseline the ICS vulnerabilities and semi-autonomously identify, respond to, and recover from asymmetric attacks on critical infrastructure in mission-relevant time frames.

Project Description:

Applies automated tools to ICS to provide:

- ICS Baseline and vulnerabilities
- Cyber & asymmetric Indications & Warnings (I&W)
- Cyber & asymmetric intrusion detection
- Semi-autonomously identify, respond to and recover from asymmetric attacks on critical infrastructure in mission-relevant timeframes

Combatant Commands' (CCMD) and SERVICES' Cyber Defenders and ICS Operators will integrate MOSAICS alerts into analytic and collection workflows



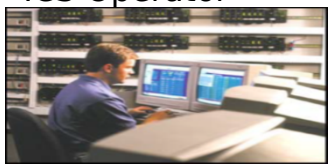
1. Establish baseline
2. Monitor for changes in equipment, network, or status
3. Threats inject malicious activity
4. Senses disruption, provide alerts
5. Provides available mitigation COA's
6. Users take action based on recommendations

MOSAICS OV1

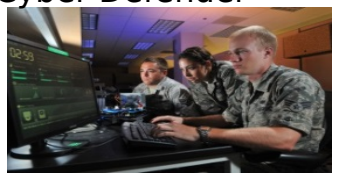
The objective of MOSAICS is to create the initial operational defense of control systems of mission critical infrastructure from cyber attacks.

ICS Protection

ICS Operator



Cyber Defender



Industrial Control Systems (ICS)

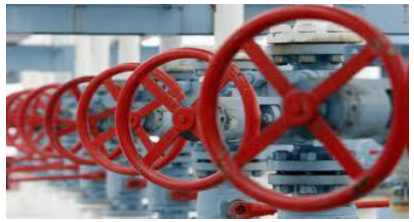
Joint Warfighter Operations

Improved Situational Awareness and Speed to Decision

Detect → Analyze → Visualize → Decide → Mitigate → Recover → Share

Smart Integration of Automation

Higher Mission Assurance



Water

Electric Grid

Fuel

Building /Plant

Protect Critical Infrastructure Industrial Control Systems from Non-Kinetic Attacks

MOSAICS Technology Approach

INL, JHU-APL, NIWC, PNNL, SNL

NAVFAC Naval Facilities Engineering Command

EXWC Engineering and Expeditionary Warfare Center

JIOR Joint Information Operations Range (JIOR) RDT&E Test Network

SCADA Supervisory Control And Data Acquisition

Note: Moved to SNL due to CR

CRAWL-WALK-RUN PROGRESSION OF COMPLEXITY

2FY19
Lab Tests

Various Labs
- Spiral 0 JHU-APL
- Table Top NAVFAC
- Integration Demo over JIOR
- Sprint Testing

1FY20
Field Test 1

NAVFAC EXWC
- Combined live network and cyber range test (SNL/EXWC hosted)
- Assess baselining and prototype capabilities in realistic electric model

4FY20
Field Test 2

NAVFAC EXWC HW-IN-THE-LOOP
- On state-of-the-art SCADA testbed at Port Hueneme, CA
- Simulated ops environment
- Participate in exercise Trident Warrior

3FY21
Military Utility Assessment (MUA)

MUA-A NAVFAC- SW OPS DEMO
- Actual application of fielded MOSAIC prototype On electrical distribution system
- Assess in operational environment under mission conditions
- IAW CONOPS & TTP
- MUA-B USAF Location
- Potential MUAs: USMC, DLA

4FY21
TRANSITION
- Fielded prototype
- CONOPS
- Updated TTPs
- Training Plans
- Industry Day
- Updated Unified Facilities Criteria
- NAVFAC POM
- HQ USAF/A4 POM
- Commercial partners
- Transition to federal sector and utilities

COTS BEST OF BREED TECHNOLOGIES & GOTS GAP FILLERS

RIGOROUS ASSESSMENT WITH REPRESENTATIVE ENVIRONMENTS AND THREATS

Program (26 October 2020)

1130-1140: Introduction
Robert Cole

1140-1200: SNL Development Team
John Jacobellis

1200-1220: SNL SCEPTRE Development Team
Chris Abate

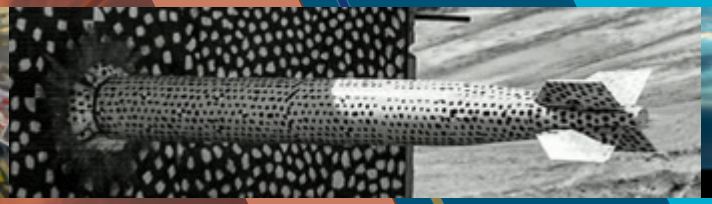
1220-1240: SNL Red Team
Tim Schulz

1240-1300: Questions

Exceptional service in the national interest








Sandia National Laboratories