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

# Autonomous Tools for Attack Surface Reduction
# Iowa State University

**Manimaran Govindarasu**

**Cybersecurity for Energy Delivery Systems Peer Review**

November 6-8, 2018

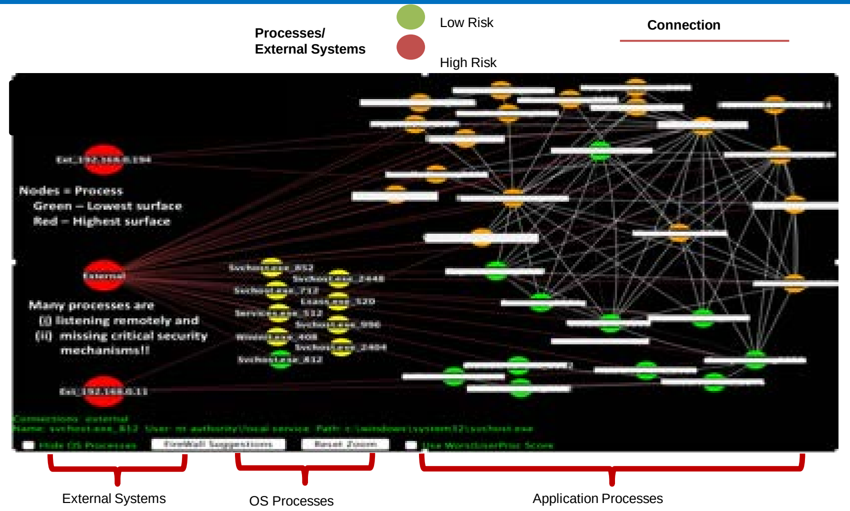
# Summary: Autonomous Tools for Attack Surface Reduction

## Objective

- Assessment and Reduction of Attack Surface within the electric power grid control environment

## Schedule

- October 1, 2016 – September 30, 2019
- Key deliverables and dates
  - Autonomous Attack Surface Reduction Framework (M2 – Tasks 2.1: Completed)
  - Attack Surface Analysis Tools & Evaluation (M3 – Tasks 2.2, 2.4: Completed)
  - Attack Surface Reduction Tools & Evaluation (M6 - Tasks 2.3, 2.4: Completed)
- What capabilities will result?
  - Attack Surface Host Analysis (AHA) Tool
  - Moving Target Defense for EDS networks
  - SIEM-based Anomaly Detection for SCADA
  - Anomaly Detection Algorithms for PMU data



Nodes = Process
Green – Lowest surface
Red – Highest surface

Many processes are
(i) listening remotely and
(ii) missing critical security mechanisms!!

Connections: external
Name: svchost.exe_812 User: nt authority\local service Path: c:\windows\system32\svchost.exe

| | |
|---|---|
| **Total Value of Award:** | **$ (1.151M + 2.981M)** |
| **Funds Expended to Date:** | **% [36.53]** |
| **Performer:** | **Iowa State University** |
| **Partners:** | **Washington State University, GE Global Research, Cedar Falls Utilities, PNNL, ANL** |

# Advancing the State of the Art (SOA)

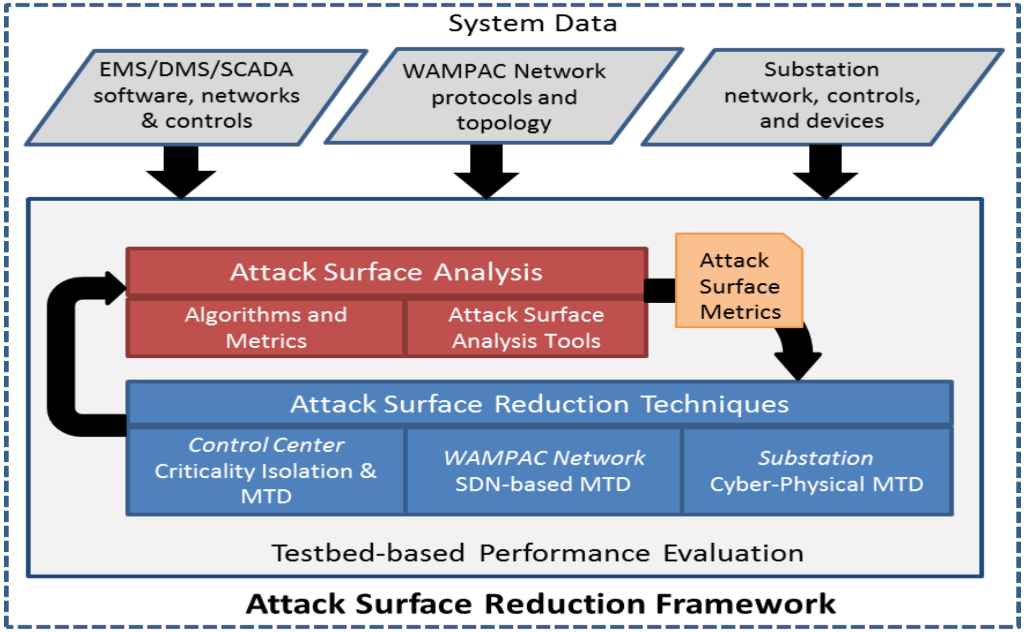
- **Describe current "state of the art"**
  EDS depends heavily on vulnerable legacy software, but there are limited tools to analyze software "attack surface"

  ICS/SCADA-specific techniques & tools are lacking

- **Describe the feasibility of your approach**
  2-stage modular architecture: coupled or decoupled deployment

  Quantitative methodology and metrics for surface analysis
  Modular techniques and toolset for attack surface reduction

- **Describe why your approach is better than the SOA**
  Most tools look primarily for "vulnerabilities", not assessing software's secure ecosystem and complexity



System Data
EMS/DMS/SCADA software, networks & controls
WAMPAC Network protocols and topology
Substation network, controls, and devices
Attack Surface Analysis
Algorithms and Metrics
Attack Surface Analysis Tools
Attack Surface Metrics
Attack Surface Reduction Techniques
Control Center Criticality Isolation & MTD
WAMPAC Network SDN-based MTD
Substation Cyber-Physical MTD
Testbed-based Performance Evaluation
Attack Surface Reduction Framework

- **Describe how the end user of your approach will benefit**
  Vendors can use AHA to improve the security lifecycle and verify good security practices

  Asset Owners can use AHA to validate the quality of software during acquisition process

  Attack Surface Reduction Tools are tailored for SCADA

- **Describe how your approach will advance the cybersecurity of energy delivery systems**

  Widespread use of AHA will address challenges of legacy software lacking adequate security protections.

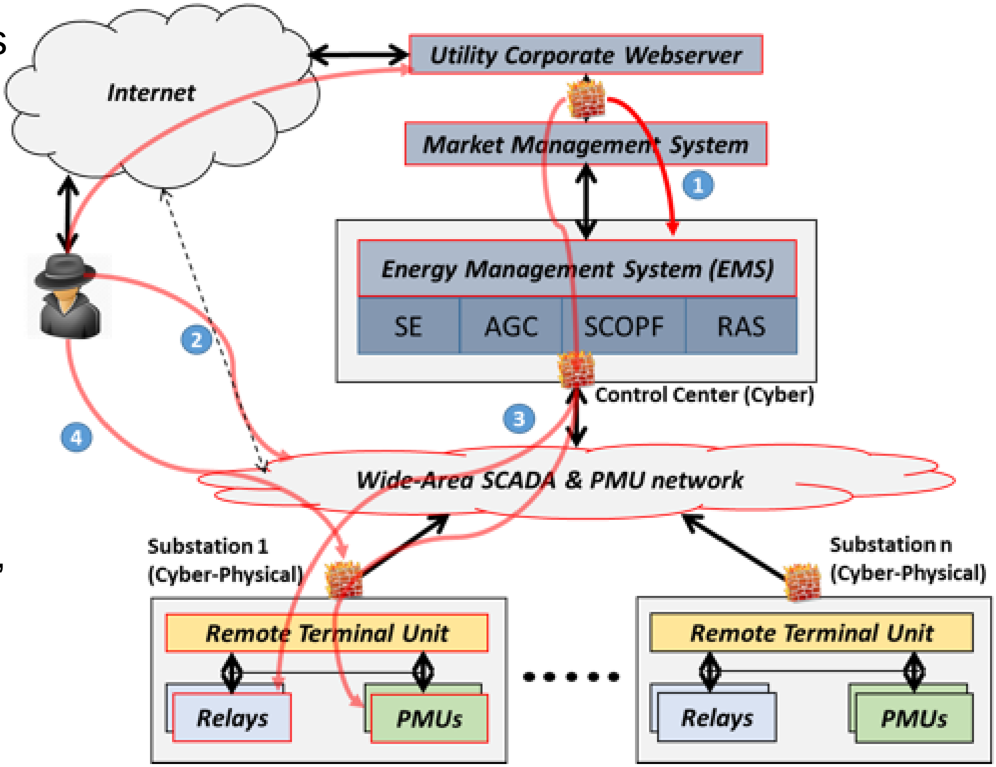
# Challenges to Success

Dynamic and evolving nature of cyber threats

Develop pragmatic methodology and metrics for attack surface analysis & reduction

- Move from qualitative approaches towards more quantitative approaches aligning with industry best practices
- Factors and complexities in analyzing and reducing attack surface for EDS
- Focus on host-based attack surface analysis, Moving Target Defense, Domain-specific Anomaly Detection to gain industry acceptance

Deployment challenges with regards to integration of cybersecurity technologies into grid’s legacy operational environments



# Scope of the RD&D Effort

## Autonomous Tools for Attack Surface Reduction

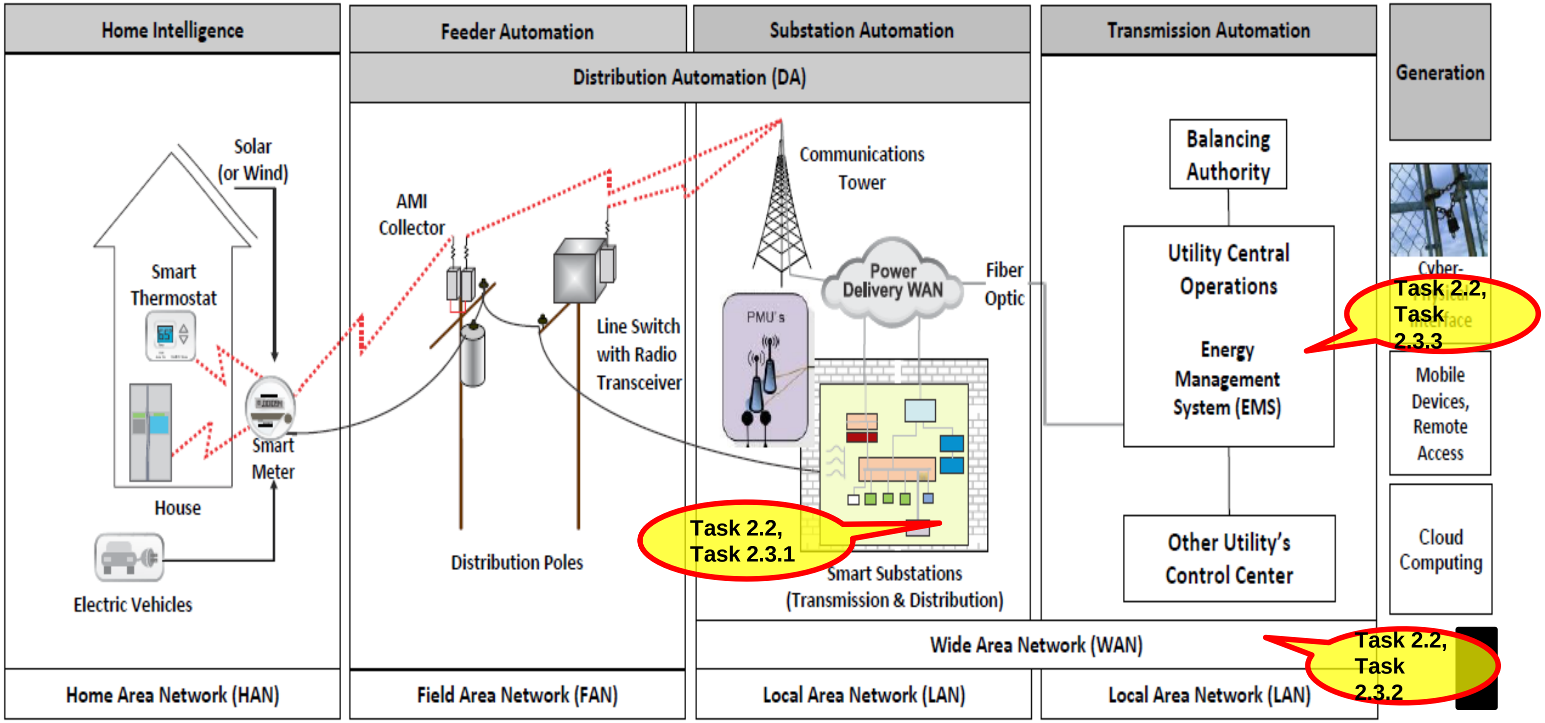


Image Credit: DOE CEDS

- **Task 2.2 –** Attack Surface Analysis algorithms and tools
- **Task 2.3.1** – Attack Surface Reduction tools at Substation level
- **Task 2.3.2** – Attack Surface Reduction tools at Wide-area Network level
- **Task 2.3.3** – Attack Surface Reduction tools at Control Center level

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

# Progress to Date

## Major Accomplishments

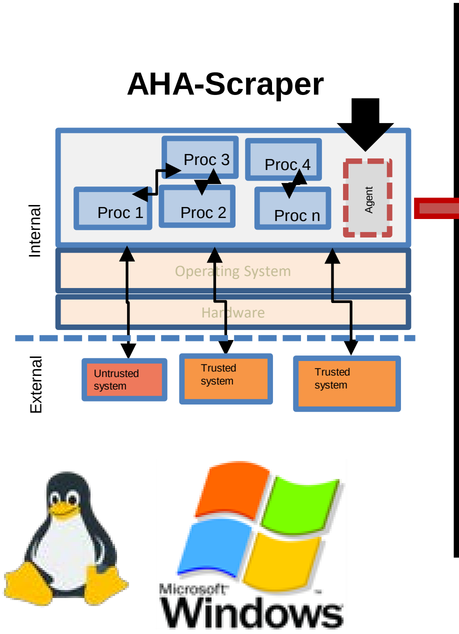
| Milestone | Completion | Verifications |
|---|---|---|
| M1. Task 1.4 – Completion of Industry Advisory Board Creation | 9/30/2017 | * Informing CEDS Project Manager of the IAB formation. |
| M2. Task 2.1 – Completion of Autonomous Attack Surface Reduction Framework | 9/30/2018 | Submitted: |
| M3. Task 2.2 – Completion of Attack Surface Analysis algorithm prototypes | 3/31/2018 | Published "Ali Tamimi, Ozgur Oksuz, Jinyoung Lee, Adam Hahn. Attack Surface Metrics and Privilege-based Reduction Strategies for Cyber-Physical Systems. 6 Jun 2018. https://arxiv.org/abs/1806.06168" |
| M4. Task 2.3 – Completion of Attack Surface Reduction algorithm prototypes | 3/31/2018 | Developed data analytic PMU attack classifier<br>Demonstrated SIEM-based ADS and firewall |
| M5. Task 2.2 – Completion of Testbed-based evaluation of Attack Surface Analysis tool and algorithm prototypes | 9/31/2018 | AHA tool published (https://aha-project.github.io) |
| M6. Task 2.3 – Completion of Testbed-based Attack Surface Reduction tool and algorithm prototype | 9/31/2018 | Testbed deployment of SIEM-based ADS<br>PMU Detection PNNL generated data sets |
| M7. Task 2.6 – Completion of Testbed-based system integration and evaluation | 9/31/2018 | AHA Outputs from assessments from 10+ EDS system on WSU/ISU/PNNL/CFU systems |
| M8. Task 3.2 – Completion of Tech transfer of prototypes to industry and utility partners | 9/31/2018 | Tool integrated into OSIsoft security evaluation processes |
| M9. Task 4.3 – Completion of Integrated system Demonstration with pilot deployments of developed tools and algorithm | 9/31/2019 | In progress.<br>Field Testing started at Cedar Falls Utilities (AHA tool and SIEM-based ADS) |

# Attack Surface Analysis

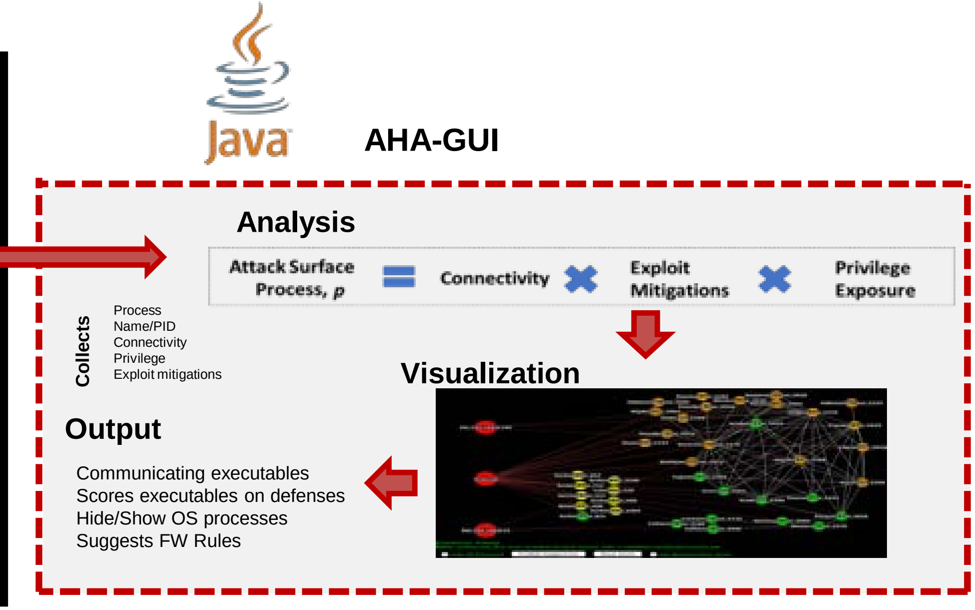
↳ AHA Tool

# Attack Surface Analysis - AHA Overview

- Analyze attack surface of critical ICS software platforms
- Provides graphical display of vulnerable processes and connections



AHA-Scraper



AHA-GUI

Analysis

Attack Surface Process, *p* = Connectivity × Exploit Mitigations × Privilege Exposure

Collects

Process Name/PID
Connectivity
Privilege
Exploit mitigations

Visualization

Output

Communicating executables
Scores executables on defenses
Hide/Show OS processes
Suggests FW Rules

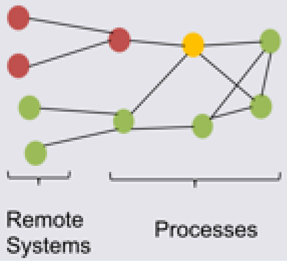
# Attack Surface Metrics

System Attack Surface $= \sum$ Process Attack Surface

Process Attack Surface $_p$ = Connectivity × Process Security × Privilege Exposure

**Remote Connectivity**

NERC CIP CIP-005-5 R1.5
(Detect suspicious comm.)



**Process Exploit Mitigation**

NERC CIP CIP-007-6 R3.1
(Prevent malicious code)

*Score(p) = f(ALSR, DEP , HighEntropyVA, ControlFlowGuard )*

**Code Integrity**

NERC CIP CIP-010-3 R1.6
(Software Integrity)

*Score(p) = f(Autenticode, StrongName)*

Refining

**Data Criticality**

Quantify impact(d) based on system contingency metrics

$Score(p) = \text{impact(data)} \quad \forall\, data \in priv(\text{p})$

TBD….

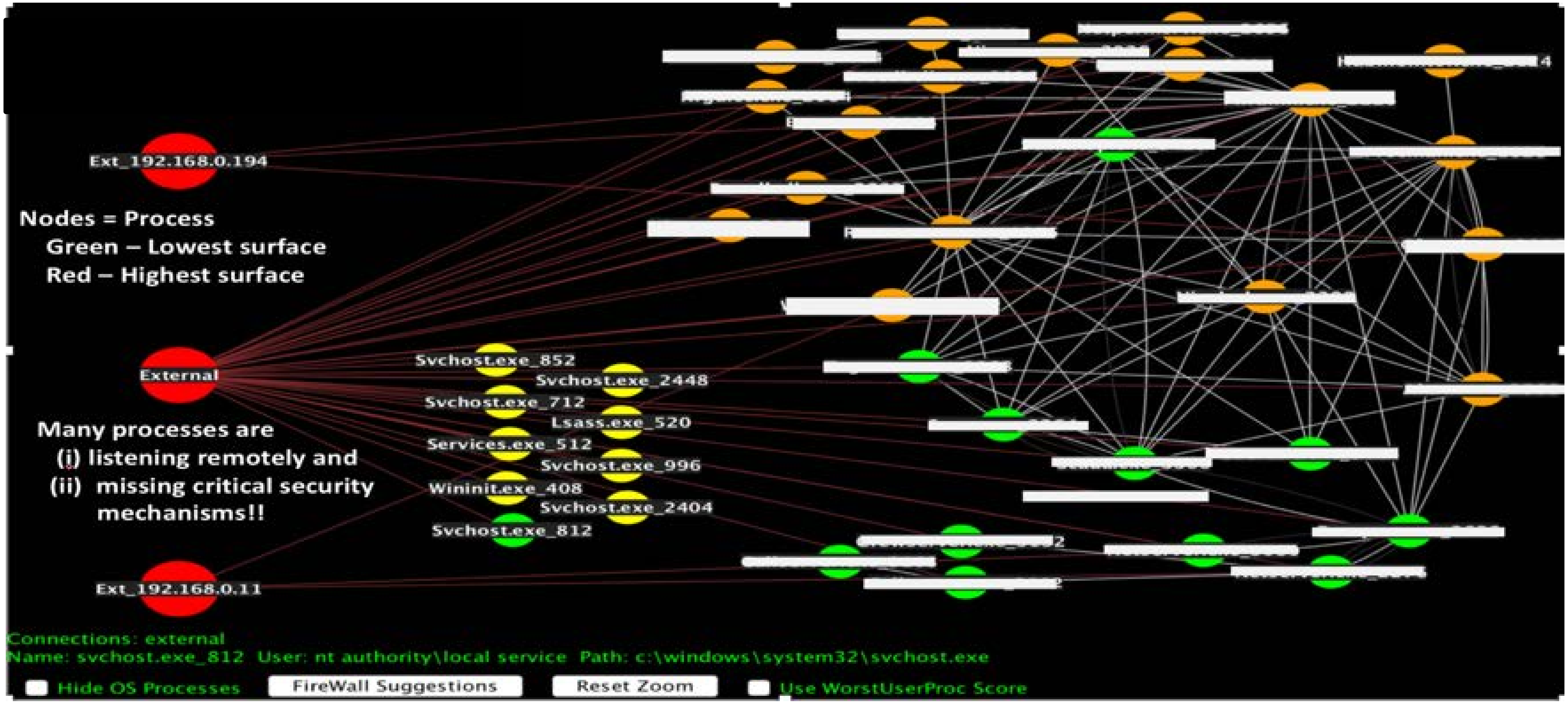
# AHA Visualization

**Processes/**
**External Systems**

● Low Risk

● High Risk

**Connection**



Nodes = Process
Green – Lowest surface
Red – Highest surface

Many processes are
(i) listening remotely and
(ii) missing critical security mechanisms!!

```
Connections: external
Name: svchost.exe_812  User: nt authority\local service  Path: c:\windows\system32\svchost.exe
```

External Systems

OS Processes

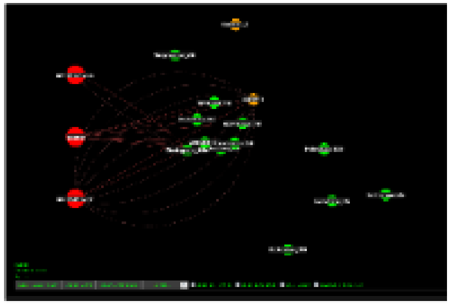
Application Processes

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

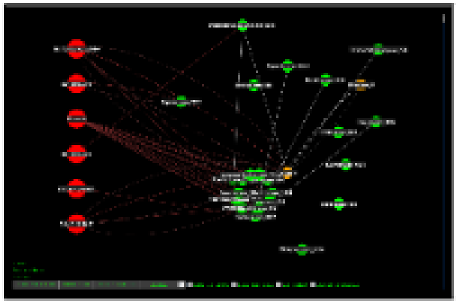
# AHA Testbed Evaluation Results

**Tool evaluated on 10+ different industry software platforms across multiple vendors**

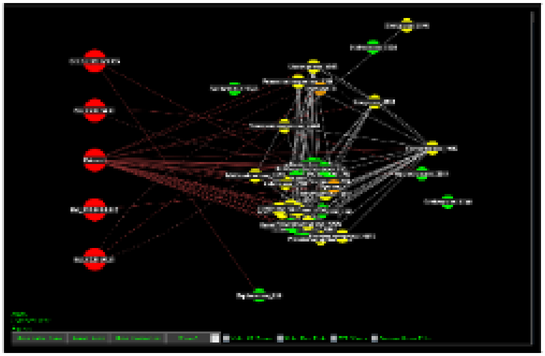
- **Locations:** WSU/PNNL/ISU/**CFU/OSIsoft**
- **Platforms**: EMS/DMS, FEPs, Historians, Substation Gateways,
- **Vendors**: GE, ABB, OSIsoft, Siemens



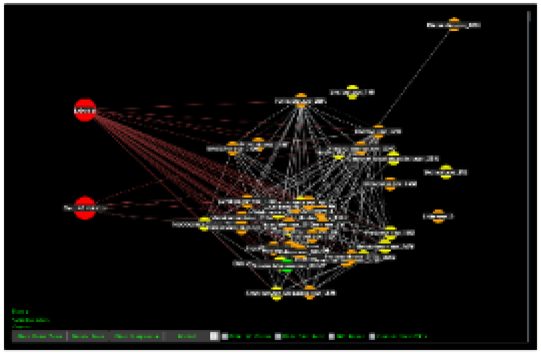
4: Historian Platform A



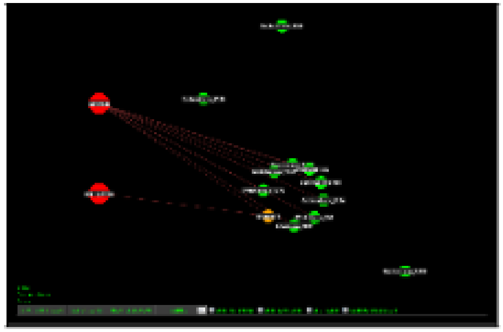
Historian Platform B



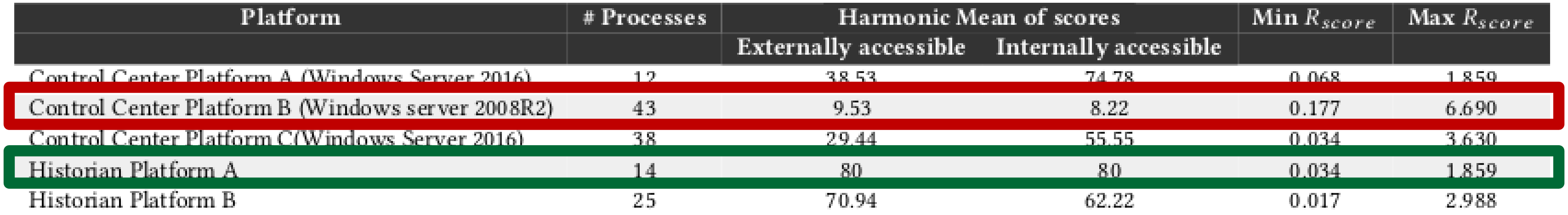
Control Center Platform A



Control Center Platform B



Control Center Platform C



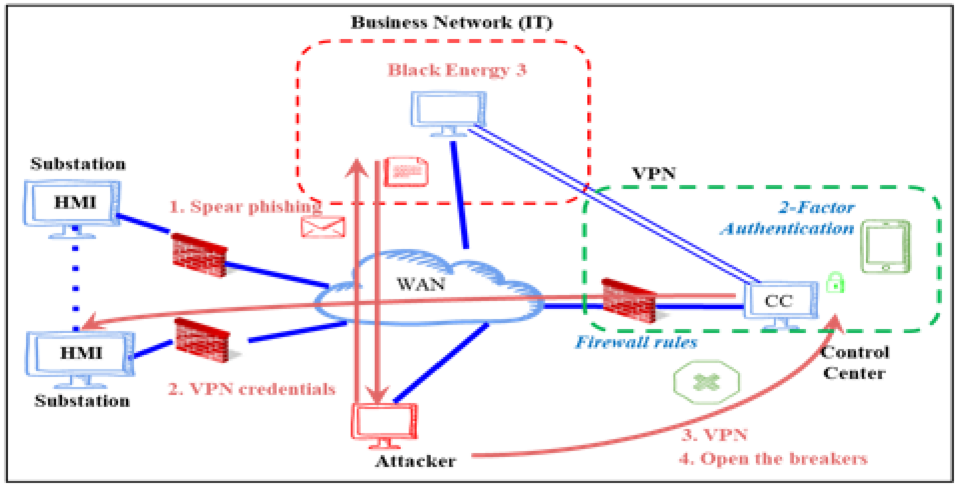
| Platform | # Processes | Harmonic Mean of scores | | Min $R_{score}$ | Max $R_{score}$ |
|---|---|---|---|---|---|
| | | Externally accessible | Internally accessible | | |
| Control Center Platform A (Windows Server 2016) | 12 | 38.53 | 74.78 | 0.068 | 1.859 |
| Control Center Platform B (Windows server 2008R2) | 43 | 9.53 | 8.22 | 0.177 | 6.690 |
| Control Center Platform C(Windows Server 2016) | 38 | 29.44 | 55.55 | 0.034 | 3.630 |
| Historian Platform A | 14 | 80 | 80 | 0.034 | 1.859 |
| Historian Platform B | 25 | 70.94 | 62.22 | 0.017 | 2.988 |

# Attack Surface Reduction

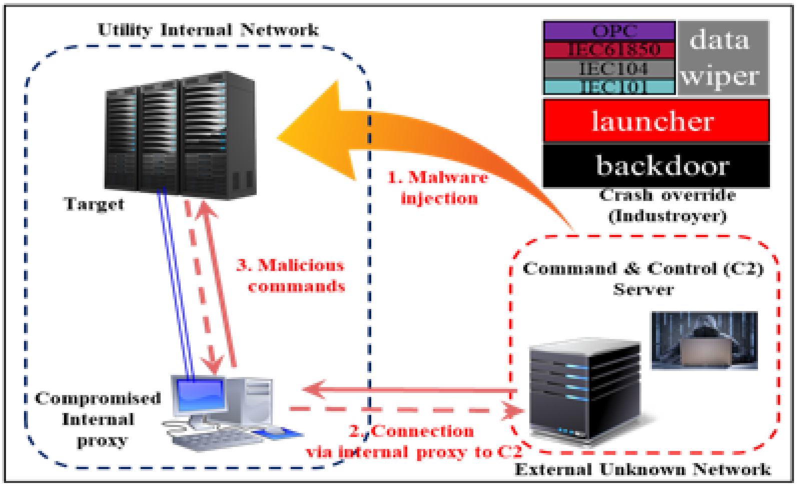
- SIEM-based ADS Design & Deployment
- Synchrophasor Fault Replay Cyber-Attack Detection Algorithm

# Attack Surface Reduction (MTD, ADS) – Real Case Studies

## *2015 Ukraine Power System Attack*



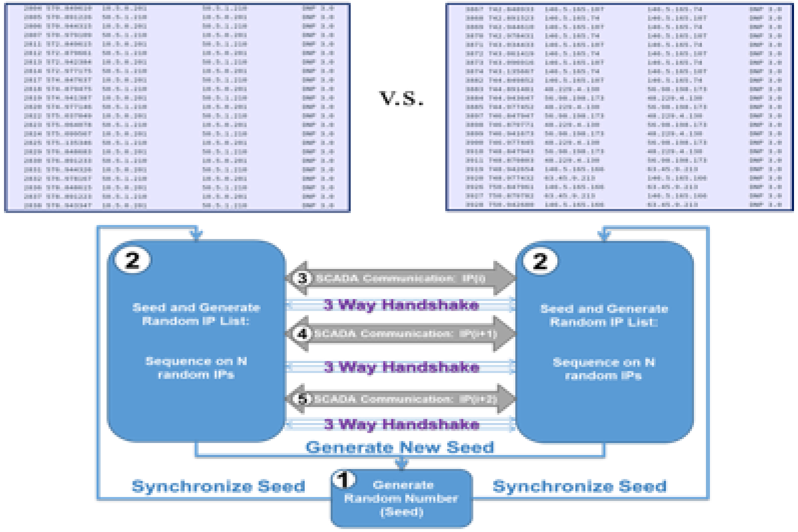
## *2016 Ukraine Power System Attack*



## *Ukraine Attacks Oriented Attack Surface Reduction*

| Events | Countermeasures | DoE CEDS Roadmap | NERC CIP |
|---|---|---|---|
| 2015 Ukraine attack | 2-factor authentication | 3: Protective Measures | CIP-005-5 R2.3: Multi-factor authentication |
| | Egress/Ingress filtering | 3: Protective Measures | CIP-005-5 R1.3: Access permissions<br>CIP-005-5 R1.5: Malicious communication detection |
| | Intrusion/Anomaly Detection | 2: Assess and Monitor Risk | |
| | Software Defined Network (SDN)+ Moving Target Defense (MTD) | 3: Protective Measures | CIP-007-5 R3.1: To deter, detect, or prevent malicious code |
| 2016 Ukraine attack | Intrusion/Anomaly Detection | 2: Assess and Monitor Risk | CIP-007-3a R4: To detect, prevent, deter, and mitigate malware |
| | SDN + MTD | 3: Protective Measures | CIP-007-5 R3.1 |

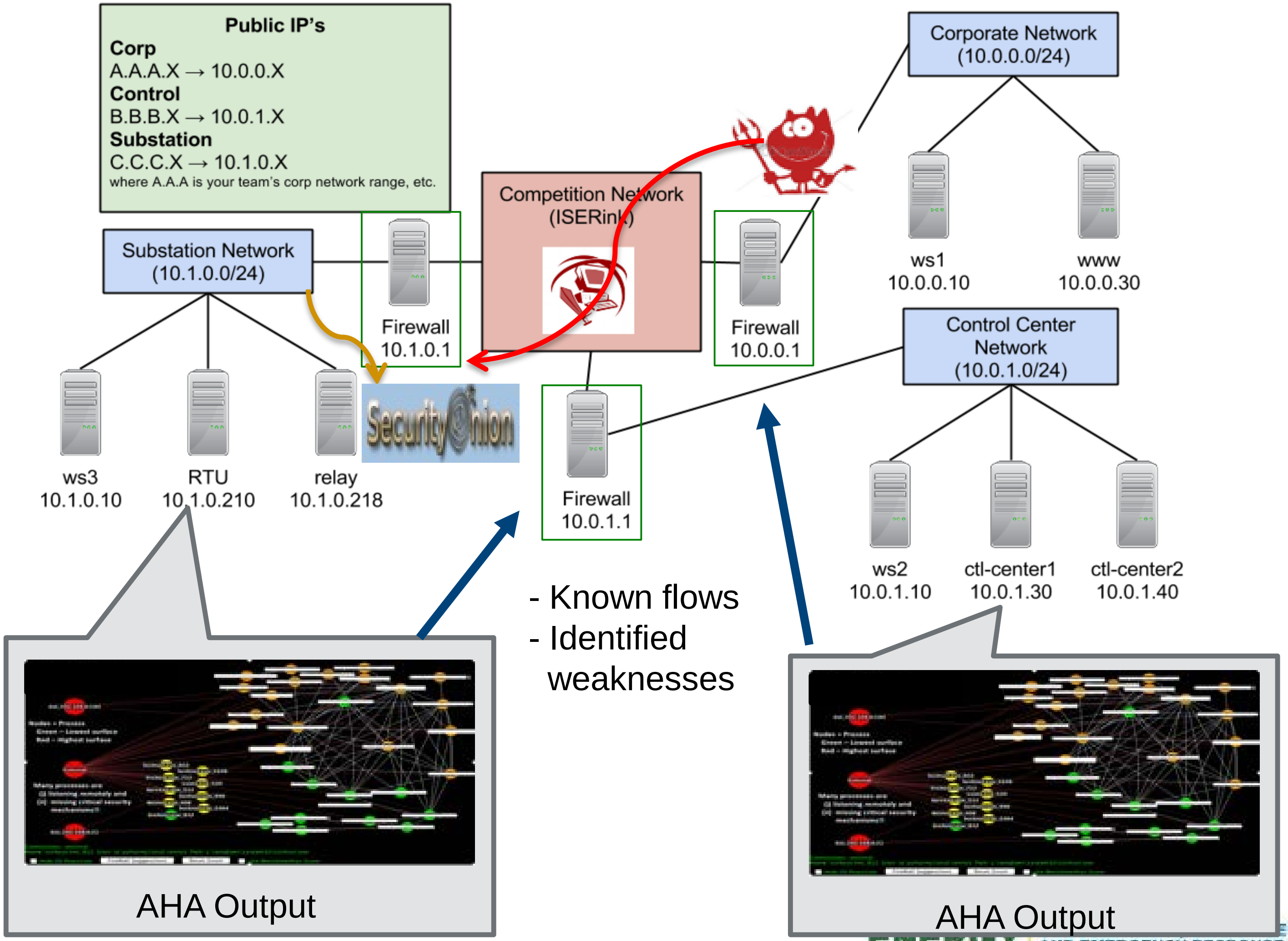
## *Moving Target Defense (MTD)*


V.S.
2
Seed and Generate Random IP List:
Sequence on N random IPs
2
Seed and Generate Random IP List:
Sequence on N random IPs
3 SCADA Communication: IP(i)
3 Way Handshake
4 SCADA Communication: IP(i+1)
3 Way Handshake
5 SCADA Communication: IP(i+2)
3 Way Handshake
Generate New Seed
Synchronize Seed
1 Generate Random Number (Seed)
Synchronize Seed

# SIEM-based ADS Design & Deployment

Attack Surface Reduction

Attack Surface Analysis



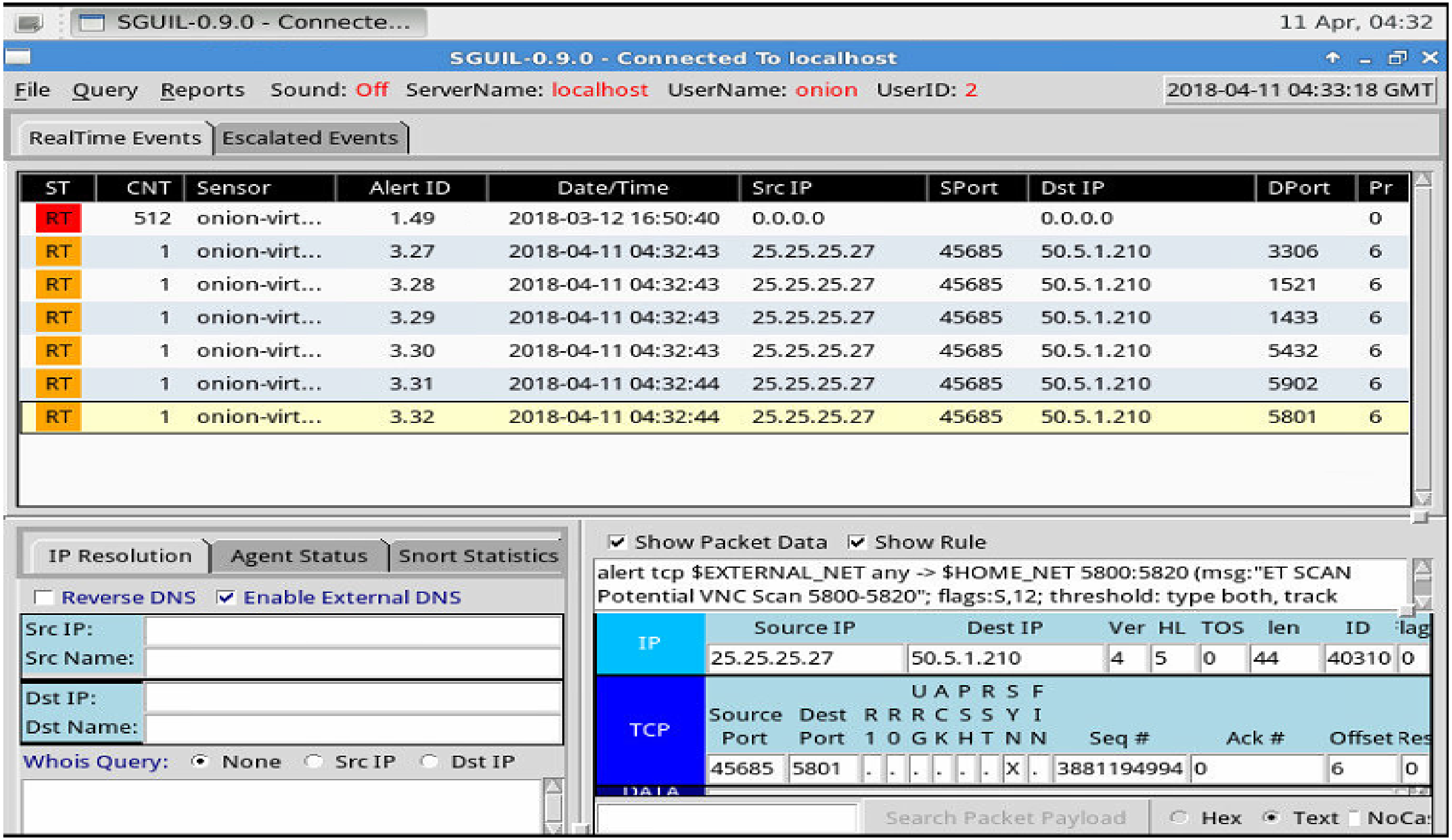
**Public IP's**
**Corp**
A.A.A.X → 10.0.0.X
**Control**
B.B.B.X → 10.0.1.X
**Substation**
C.C.C.X → 10.1.0.X
where A.A.A is your team's corp network range, etc.

- Known flows
- Identified weaknesses

AHA Output

AHA Output

# SIEM-based IDS/ADS in substation network – ping scan detection



Sound: Off ServerName: localhost UserName: onion UserID: 2 2018-04-11 04:33:18 GMT

| ST | CNT | Sensor | Alert ID | Date/Time | Src IP | SPort | Dst IP | DPort | Pr |
|---|---|---|---|---|---|---|---|---|---|
| RT | 512 | onion-virt... | 1.49 | 2018-03-12 16:50:40 | 0.0.0.0 | | 0.0.0.0 | | 0 |
| RT | 1 | onion-virt... | 3.27 | 2018-04-11 04:32:43 | 25.25.25.27 | 45685 | 50.5.1.210 | 3306 | 6 |
| RT | 1 | onion-virt... | 3.28 | 2018-04-11 04:32:43 | 25.25.25.27 | 45685 | 50.5.1.210 | 1521 | 6 |
| RT | 1 | onion-virt... | 3.29 | 2018-04-11 04:32:43 | 25.25.25.27 | 45685 | 50.5.1.210 | 1433 | 6 |
| RT | 1 | onion-virt... | 3.30 | 2018-04-11 04:32:43 | 25.25.25.27 | 45685 | 50.5.1.210 | 5432 | 6 |
| RT | 1 | onion-virt... | 3.31 | 2018-04-11 04:32:44 | 25.25.25.27 | 45685 | 50.5.1.210 | 5902 | 6 |
| RT | 1 | onion-virt... | 3.32 | 2018-04-11 04:32:44 | 25.25.25.27 | 45685 | 50.5.1.210 | 5801 | 6 |

☐ Reverse DNS ☑ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: ● None ○ Src IP ○ Dst IP

☑ Show Packet Data ☑ Show Rule

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 5800:5820 (msg:"ET SCAN
Potential VNC Scan 5800-5820"; flags:S,12; threshold: type both, track
```

| | Source IP | Dest IP | Ver | HL | TOS | len | ID | lag |
|---|---|---|---|---|---|---|---|---|
| IP | 25.25.25.27 | 50.5.1.210 | 4 | 5 | 0 | 44 | 40310 | 0 |

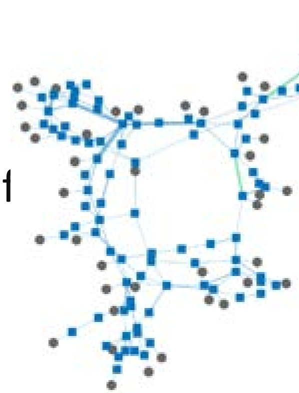
| | Source Port | Dest Port | R 1 | R 0 | U R G | A C K | P S H | R S T | S Y N | F I N | Seq # | Ack # | Offset | Res |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| TCP | 45685 | 5801 | . | . | . | . | . | . | X | . | 3881194994 | 0 | 6 | 0 |

○ Hex ● Text ☐ NoCa

# Synchrophasor Fault Replay Cyber-Attack Detection Algorithm (GE GRC)

- Algorithm addresses adversarial spoofing of PMU data
- Reduces key attack vector entry point into EMS apps
- Data-driven, but feature selection motivated by physical model;  easy to train

Transmission System:



*PMU Data*

*(System Info)*

PMU “Firewall”

*Alarm*

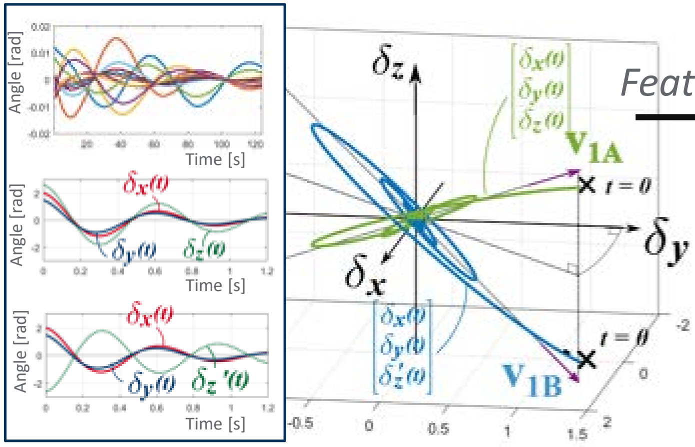
*Hardened PMU Data*

Control Center:

GE Grid Solutions WAMS Applications

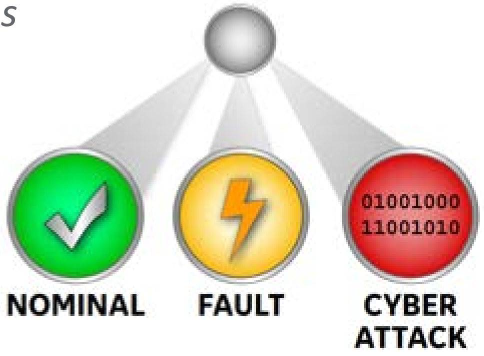
## Synchrophasor Spoofing Detection Algorithm

*SVD & Power Systems Analytics:*

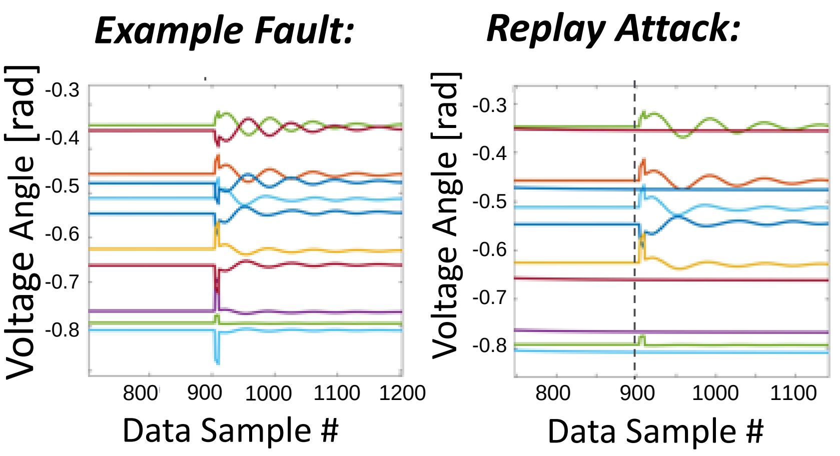


*Features*

*Rapid Detection and Classification:*



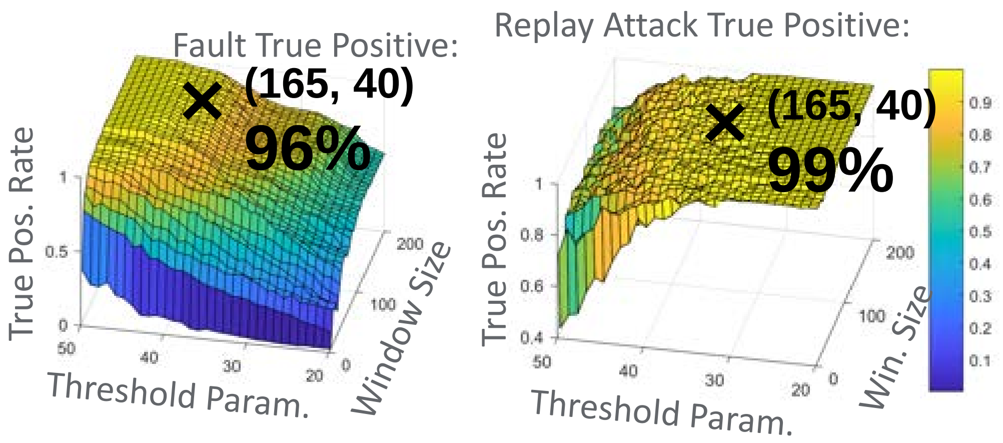
# Performance of Fault Replay Cyber-Attack Detection Algorithm (GE GRC)



***Example Fault:***

***Replay Attack:***

## *1 Event in Repository; 2/11 PMUs Compromised:*



Fault True Positive:

(165, 40)

96%

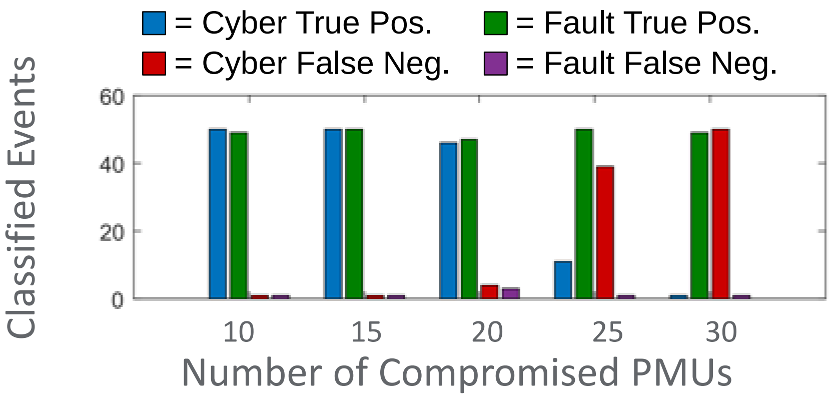
Replay Attack True Positive:

(165, 40)

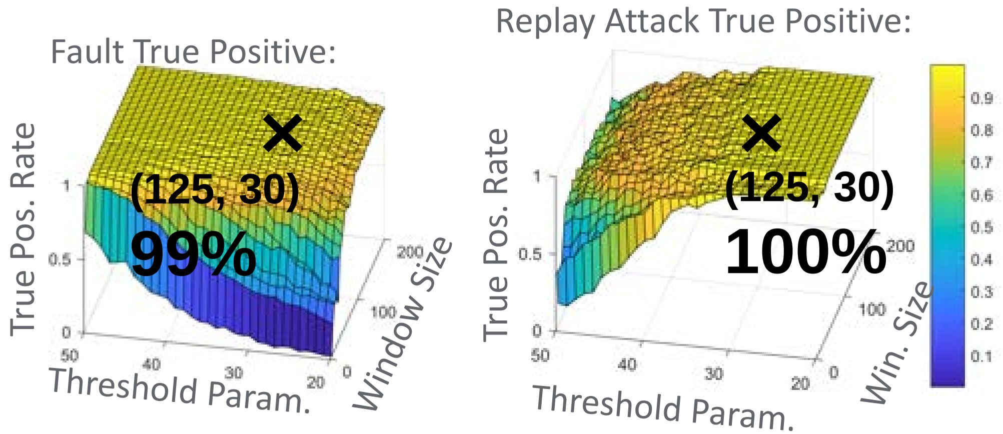
99%

## *Validation using PNNL Testbed Data:*

WECC System; PMUs at 30/63 buses;
100 Scenarios Repeated 5x:



## *3 Events in Repository; 2/11 PMUs Compromised:*



Fault True Positive:

(125, 30)

99%

Replay Attack True Positive:

(125, 30)

100%

High true pos. rate, validated with help of PNNL; integration with GEGS EMS in Phase II

# Collaboration/Technology Transfer

## OSISoft

**Internal:** Integration with SDLC for Windows/Linux/Cloud environments

**External**: Recommended for OSI System Hardening

github.com/hpaul-osi/HardenedBaselines (Security Policy Configuration Tools)

## Tech Transfer

https://aha-project.github.io/

AttackSurface Host Analyzer

Repository for the documentation website

Project maintained by aha-project | Hosted on GitHub Pages — Theme by mattgraham

About AHA

AHA is a suite of tools, presently this is two halves, the scraper component available for Linux or Windows which gathers the information, and AHA-GUI visualizer which displays the results of the scraper.

Using AHA-Scraper

Running on Windows

Dependencies

The Windows AHA-Scraper has no real dependencies, but presently only works on x86_64. 32bit support will be added at some future date.

Usage

use git clone, the github client, or click 'download project' to get the repository on your computer. Then cd into the directory and run:

### Cedar Falls Utilities (Summer/Fall 2018)

**SIEM-ADS: Prelim Deployment and Testing of ICS Anomaly-Detection System**

**MTD: Feasibility evaluation for deployment (Layer 3 vs. Layer 2 solution)**

### Alliant Energy (Summer 2018)

**SIEM-ADS: Training module on ICS/SCADA Anomaly-Detection System**

### Idaho Power (Summer 2018)

**SIEM-ADS: Training module on ICS/SCADA Anomaly Detection System**

### NERC GridSecCon (Fall 2018)

**SIEM-ADS: Training module on ICS/SCADA Anomaly Detection System**

### Iowa State University – Graduate Research & Education

**SIEM-ADS: Deployment and Testing of ICS Anomaly-Detection System**

**MTD: Testbed-based implementation, testing, and evaluation**

# Collaboration/Technology Transfer

## Plans to transfer technology/knowledge to end user

**•Increase industry acceptance of AHA Tool among vendors and asset owners**

- Presentations to more industry events
- Aggressively identify perspective vendor and asset owner users to evaluate AHA
- Explore Commercialization Opportunities for AHA tool

**•Adoption of SIEM-based ADS into Utility SCADA Environment**

- Cedar Falls Utilities, CornBelt Coop, MISO, MidAmerican, Alliant Energy

**•Adoption of Layer 2 MTD in Utility SCADA Environment**

- Cedar Falls Utilities

**•Hosting/Hosted Testbed-based training sessions**

- Utilities within Iowa and beyond (Idaho Power, MISO), GridSecCon 2018 …

**•Adoption of Attack Surface Analysis and Reduction Techniques/Tools by EMS Vendors**

- OSISoft (adopted AHA tool) and GE Grid Solutions (potentially)

# Next Steps for this Project

## Phase II: Field Deployment, Testing, Evaluation, Tech Transfer

### Attack Surface Analysis Tool (WSU, GE-GR, PNNL)

- Incorporate system interconnections (e.g., network of systems into AHA)
- Incorporate system metrics into incorporate grid physical system metrics
- Evaluate AHA performance on additional EDS platforms

### Attack Surface Reduction Tool (ISU, CFU, GE, ANL)

- SIEM-ADS Tool deployment, testing, and evaluation at Cedar Falls Utilities
- SIEM-ADS Tool via Training Session for MISO and CornBelt Power Coop
- Layer 2 Deployment, Testing and Evaluation at Cedar Falls Utilities
- PMU-based Anomaly Detection Algorithms & Integration into GE EMS Platform