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

Cybersecurity Center for Secure, Evolvable Energy Delivery Systems (SEEDS)

University of Arkansas

H. Alan Mantooth, Qinghua Li

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Summary: Cybersecurity Center for Secure, Evolvable Energy Delivery Systems (SEEDS)

Objective

- Research and develop cybersecurity technologies, tools, and methodologies that will advance the energy sector's ability to survive cyber attacks and incidents while sustaining critical functions
- Scope of work: cybersecurity of power electronics, data, operation and control systems, and operation networks in energy delivery systems

Schedule

- Project start/end dates: 10/01/2015 – 09/30/2020
- Deliverables: cybersecurity technologies well designed, implemented, and tested
- Security capabilities that result from research projects of this center: threat and risk assessment; incident prevention, detection, mitigation, and response; defense in depth against dynamic threats; security management and decision support

Total Value of Award:	**$12,226,504+$3,082,610**
Funds Expended to Date:	**%52**
Performer:	**University of Arkansas**
Partners:	**Arkansas Electric Cooperative Corporation Carnegie Mellon University Florida International University Lehigh University Massachusetts Institute of Technology University of Arkansas, Little Rock**

Advancing the State of the Art (SOA)

- **State of the art (SOA)**
  - Power grid control and operation systems and operation technology infrastructure need better and customized protection against cyber threats
  - New power grid components and services are usually deployed first and then security is validated and added later
  - Cybersecurity management is mostly manual
  - Gap between fundamental research and technology transfer to industry
- **Our approach**
  - Provides protection against cyber attacks based on computing methods and the physics of energy delivery systems
  - Industry inputs throughout the R&D cycle (define, research, alpha, beta, transition)
  - Yearly solicitation of security problems from industry and proposals from faculty
- **Why our approach is better than the SOA**
  - Customized protection for energy delivery systems
  - Builds security into the design of new power grid components and services
  - Security management automation to tackle the high complexity and volume of security data
  - Our security solutions are more practical for deployment

Advancing the State of the Art (SOA)

- **Feasibility of approach**
  - Involvement of industry in the entire cycle, including needs solicitation, project selection, feedback to research, and beta testing
  - Technology intentionally made easy-to-integrate into the existing system, e.g., avoiding interruption of service
- **How the end user will benefit**
  - All research is industry-driven and research solution efficacy is validated for transition to practice and commercialization
  - Research university partners have testing facilities to evaluate cybersecurity tools prior to deployment
  - Research is beta tested with an energy industry partner
  - The intense research and development focus allows for the involvement of students from all partner institutions to help provide industry a robust cybersecurity workforce
- **How our approach will advance the cybersecurity of energy delivery systems**
  - Improve situational awareness through *security data analytics and anomaly detection*
  - Protect integrity of operation and control by *hardening hardware, detecting tempering of data and devices*
  - Secure communication network infrastructure by *designing secure extensions to standard communication protocols and detecting network attacks*
  - Advance security management by *providing automation technologies and decision support*

Challenges to Success

Challenge 1: Solutions need knowledge from both cybersecurity and power systems, and from both academe and industry

- Bridge the gap between industry and academe
- Interdisciplinary team across cybersecurity, computer science, and power systems

Challenge 2: Difficult to obtain industry data

- Involving industry partners more closely
- Working with industry to sanitize data
- Sending student interns to industry partners

Challenge 3: Integration into existing systems without interrupting service

- Account for the impact of solutions on the existing system in design and evaluation
- Beta testing at industry partners or over industry-shared data

Challenge 4: Center sustainability

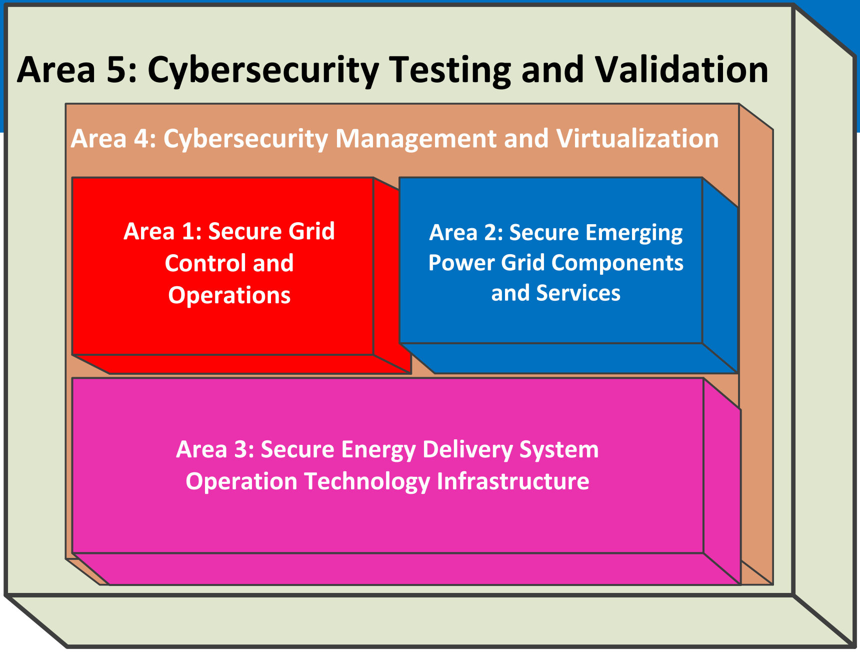
- Continue to provide benefits that convince industry to join the center
- Multi-tier membership structure to provide flexibility to members

Progress to Date (1/2)

Major Accomplishments

- 15 cybersecurity tools developed and tested
- 6 inventions disclosed
- 30 journal publications
- 54 conference publications
- 11 more papers in submission
- 10 invited talks
- 1 cybersecurity special section at IEEE Journal of Emerging and Selected Topics in Power Electronics
- 1 Cybersecurity Session at IEEE ECCE 2016
- Collaboration with ORNL to organize a cyber conference
- 6 industry engagement meetings
- Evaluative methodology for project selection
- 8 Industrial Board Members as a paying organization - to fund additional efforts
- 60 organizations that SEEDS has interacted with
- 48 students

Progress to Date (2/2)


Area 5: Cybersecurity Testing and Validation
Area 4: Cybersecurity Management and Virtualization
Area 1: Secure Grid Control and Operations
Area 2: Secure Emerging Power Grid Components and Services
Area 3: Secure Energy Delivery System Operation Technology Infrastructure

Major Accomplishments

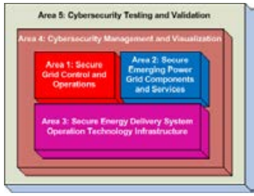
- Automating remediation action analysis for security vulnerabilities
- Detecting compromised devices through system call tracing
- Detecting payload attacks through time-based physical side channels
- Detecting and localizing data falsification attacks in AGC through learning-based and physics-based methods
- Joint detection of data integrity attacks and resilient power state estimation
- Active detection of data integrity attacks
- Detecting and localizing topology attacks through hypothesis testing
- Quickest detection of sparse false data injection attacks
- Detecting unidentifiable false data injection attacks
- Sequence hopping-based fast authentication for IEC 61850 GOOSE messages
- Detecting Botnet in SCADA networks
- Detecting stealthy, low-rate flooding attacks in time-critical communications
- Bloom filter-based public key management for smart meter networks
- Detecting time synchronization attacks against PMU data
- More to come

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Targeted end user for the technology: both vendors and facility owners
  - Vendors: customized intrusion detection technologies, data forgery detection tools, security data analytics tools
  - Facility owners: cybersecurity management and visualization tools, situational awareness tools
- Plans to gain industry acceptance
  - Security needs take input from industry
  - Project selection suggested by industry
  - Technology design takes feedback via industry focus group activities
  - Beta testing of technologies conducted at industry partner AECC, EPRI, other facilities available, or over industry data
  - Communications to industry through avenues in addition to academic publications

Next Steps for SEEDS (1/3)



Area 5: Cybersecurity Testing and Validation

Area 4: Cybersecurity Management and Visualization

Area 1: Secure Grid Control and Operations

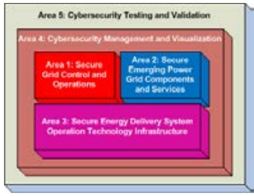
Area 2: Secure Emerging Power Grid Components and Services

Area 3: Secure Energy Delivery System Operation Technology Infrastructure

Approach for the next year or to the end of project

- Early Insider Threat Detection
- Detection and Mitigation of Cyber Physical Systems-Based Attacks on Natural Gas Delivery Systems
- Enhancing Resilience of Field Devices under Payload Attacks
- Detecting Compromised Devices
- Topology Attacks
- Countering Data Integrity Attacks
- Quickest Intrusion Detection
- Cyber-Secure Power Router
- Misuse of DSM

Next Steps for SEEDS (2/3)


Area 5: Cybersecurity Testing and Validation
Area 4: Cybersecurity Management and Visualization
Area 1: Secure Grid Control and Operations
Area 2: Secure Emerging Power Grid Components and Services
Area 3: Secure Energy Delivery System Operation Technology Infrastructure

Approach for the next year or to the end of project

- Lightweight Key Management for Low-bandwidth Legacy Environments in Smart Grid
- Intrusion and Botnet Detection in SCADA
- Securing IEC 61850 Layer 2 GOOSE Messages
- Automated Security Vulnerability and Patch Management
- Extended Cybersecurity Threat Information Sharing
- A Tri-Modular Framework for an Intelligent Visualization of Smart Grid Cyber-Attacks
- Continuing proposal solicitation and selection

Next Steps for SEEDS (3/3)

- Transition of mature tools to practice
- We have expanded collaboration with industry, national labs in proposal submissions and will continue collaborations in various ways
- Grow industry memberships for sustainability
- Continue to involve additional researchers
- Expand center-based activities

Sample Project: Security Vulnerability Automated Remediation Tool (SPARTAN) [PI: Qinghua Li, UA]

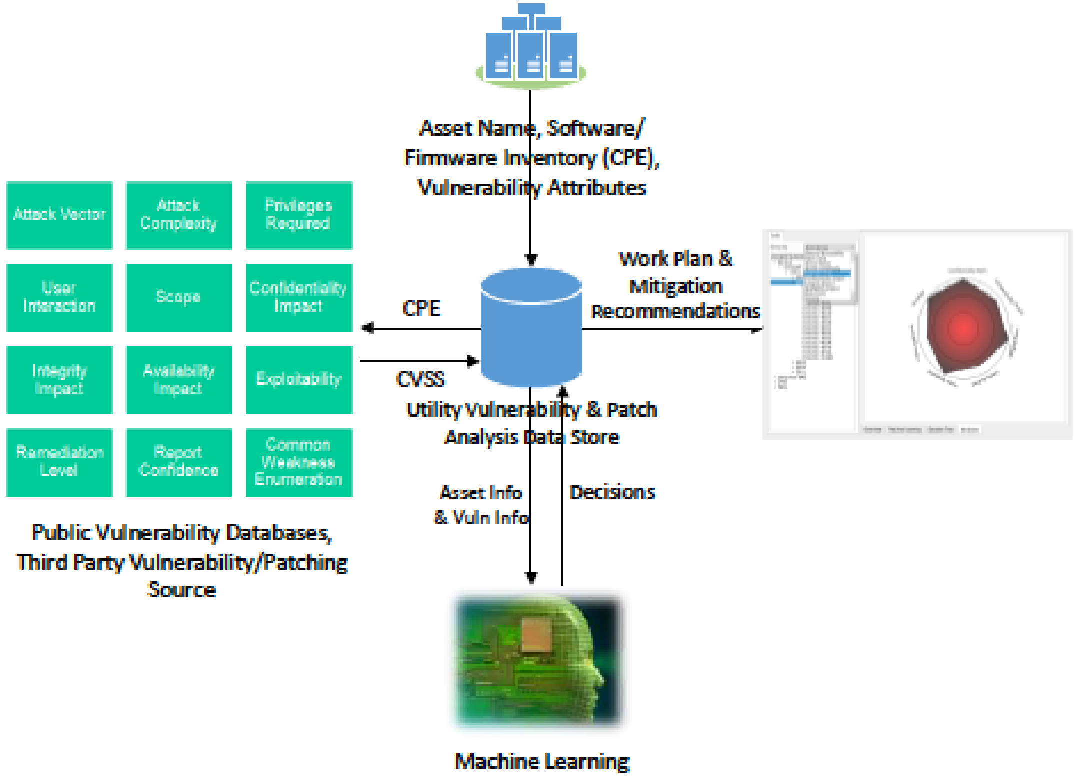
Problem

Security vulnerability and patch management is a heavily manual process. Remediation action analysis for each and every vulnerability consumes much time, causes long remediation delays, and increases risks

Achievements

SPARTAN automates remediation analysis through machine learning to remediate vulnerabilities more timely and reduce risks of exploits

Tests over a one-year dataset from a utility partner show high performance



Attack Vector
Attack Complexity
Privileges Required
User Interaction
Scope
Confidentiality Impact
Integrity Impact
Availability Impact
Exploitability
Remediation Level
Report Confidence
Common Weakness Enumeration

Public Vulnerability Databases, Third Party Vulnerability/Patching Source

Asset Name, Software/ Firmware Inventory (CPE), Vulnerability Attributes

CPE

CVSS

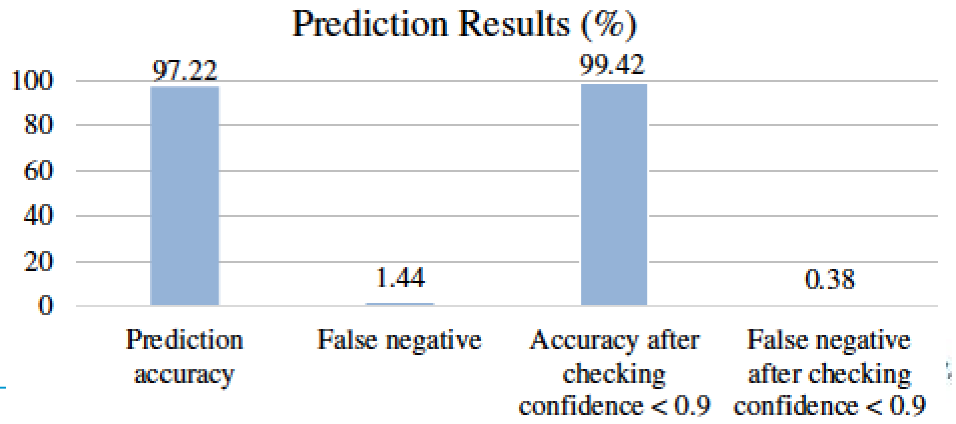
Utility Vulnerability & Patch Analysis Data Store

Work Plan & Mitigation Recommendations

Asset Info & Vuln Info

Decisions

Machine Learning



Sample Project: Cyber Secure Power Router [PI: H. Alan Mantooth, UA]

Problem Addressed:

Defense-in-Depth for
Grid Operational Technology

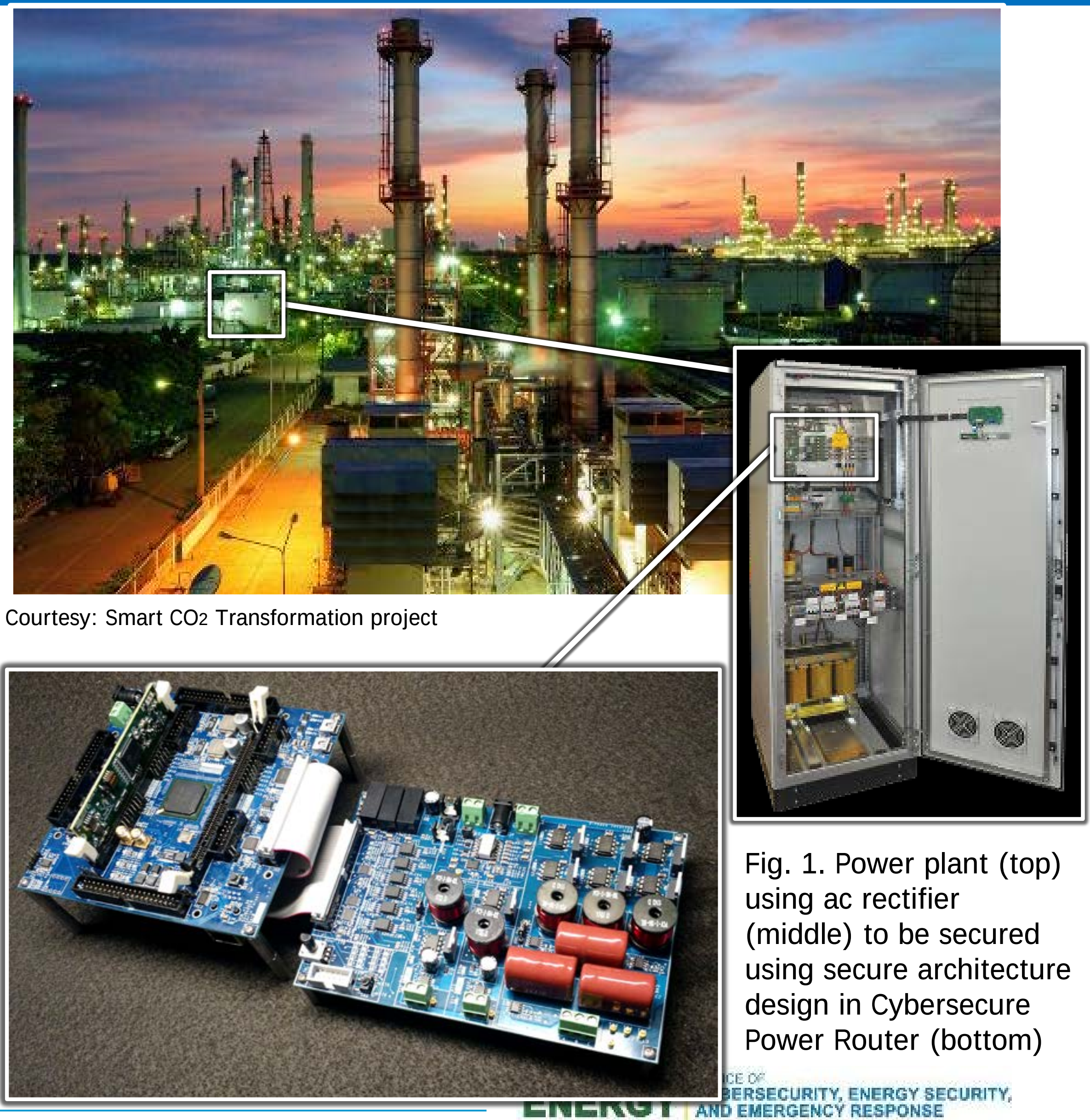
Achievements:

- Secure Architecture Design
- Hot-Patching Technique
- Encrypted Communication
- Hardware Assisted Monitoring

Industry Relevance:

Improved Cybersecurity for

- Industrial Control Systems
- Converters
- Photovoltaic Inverters
- Motor Drives
- Active Rectifiers
- Telemetry/Smart Meters



Courtesy: Smart CO_2 Transformation project

Fig. 1. Power plant (top) using ac rectifier (middle) to be secured using secure architecture design in Cybersecure Power Router (bottom)

Sample Project: Sequence Hopping Algorithm for Secure GOOSE Messages [PI: Osama Mohammed, FIU]

What is the product?

Sequence Hopping Algorithm to protect IEC 61850 GOOSE messages against attacks.

Deployment

Alpha tested V1.0 of Sequence Hopping Algorithm for protecting Layer 2 GOOSE Messages at FIU Smart Grid Testbed.

Beta tested V1.0 of Sequence Hopping Algorithm for protecting Layer 2 GOOSE Messages at Electric Power Research Institute (EPRI), in Knoxville, TN.

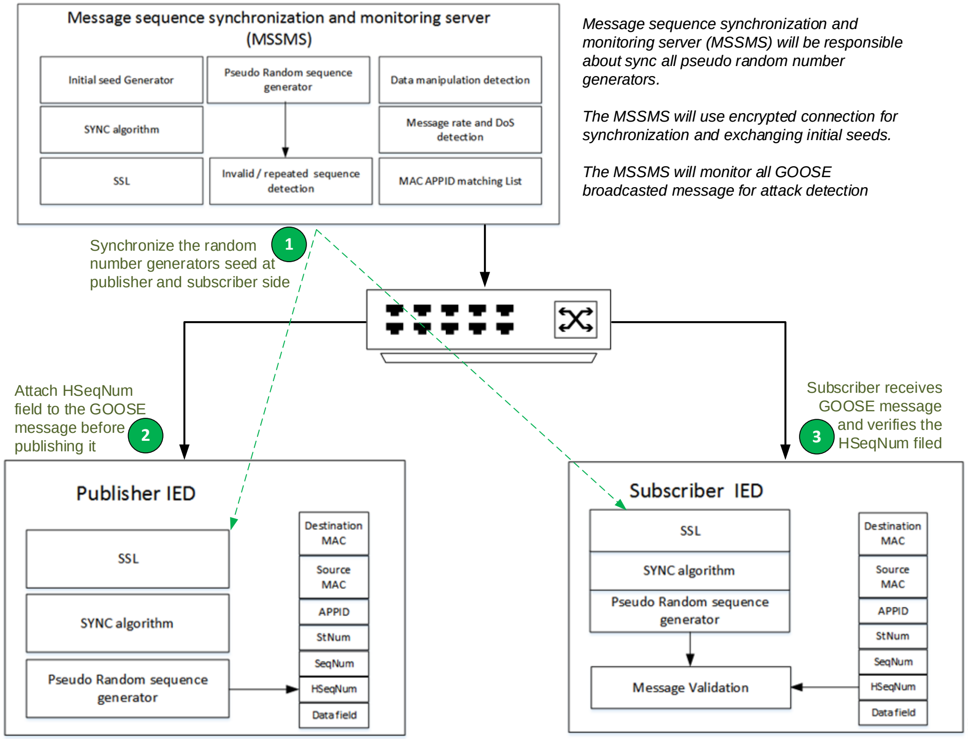
A US Patent (9894080) has been awarded for the efforts completed so far.

This solution could be deployed through a firmware update to IEDs or as a bump-in-the-wire device.

Industry Relevance

Addressing the security of critical IEC 61850 GOOSE messaging protocol, which is a widely accepted standards.

Presented the research efforts in the IEC TC57 WG15 meeting in May, 2018.



Message sequence synchronization and monitoring server (MSSMS)

Initial seed Generator

Pseudo Random sequence generator

Data manipulation detection

SYNC algorithm

Message rate and DoS detection

SSL

Invalid / repeated sequence detection

MAC APPID matching List

1 Synchronize the random number generators seed at publisher and subscriber side

2 Attach HSeqNum field to the GOOSE message before publishing it

3 Subscriber receives GOOSE message and verifies the HSeqNum filed

Publisher IED

SSL

SYNC algorithm

Pseudo Random sequence generator

Destination MAC

Source MAC

APPID

StNum

SeqNum

HSeqNum

Data field

Subscriber IED

SSL

SYNC algorithm

Pseudo Random sequence generator

Message Validation

Destination MAC

Source MAC

APPID

StNum

SeqNum

HSeqNum

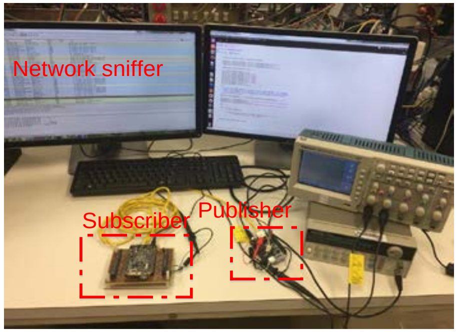
Data field

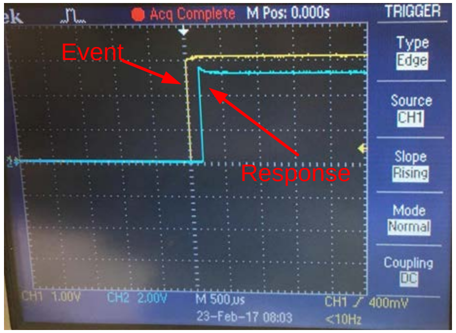
Message sequence synchronization and monitoring server (MSSMS) will be responsible about sync all pseudo random number generators.

The MSSMS will use encrypted connection for synchronization and exchanging initial seeds.

The MSSMS will monitor all GOOSE broadcasted message for attack detection

Experimental Validation

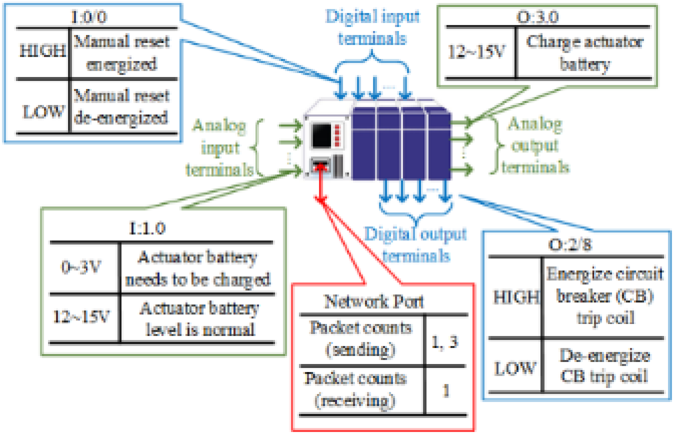




End-to-end delay time for the embedded sequence hopping implementation is **250 micro seconds**

Sample Project: Detecting PLC Payload Attacks on Field Devices [PI: Mooi Choo Chuah, Lehigh University]

- **Objective:** Field devices are subjected to payload attacks where attackers modify control program payload to execute malicious logics. Our goal is to design an efficient scheme that detects such attacks.
- **Technical Approach:** Runtime behavior model of legitimate PLC control program is built and PLC firmware is modified to monitor such runtime behaviors so as to detect any abnormality.
- **Accomplishments:** Completed Alpha testing of the proposed detection mechanism of firmware level PLC payload attacks at NCREPT; the results show that our approach can detect payload attacks (see Fig. 2).
- **Deployment:** Our proposed kernel-level enhancements can be incorporated into the firmware offered by PLC manufacturers. The detection mechanism design follows a widely-used PLC program execution model, minimizing software architectural changes required by deployment.



I:0/0	
HIGH	Manual reset energized
LOW	Manual reset de-energized

O:3.0	
12~15V	Charge actuator battery

I:1.0	
0~3V	Actuator battery needs to be charged
12~15V	Actuator battery level is normal

Network Port	
Packet counts (sending)	1, 3
Packet counts (receiving)	1

O:2/8	
HIGH	Energize circuit breaker (CB) trip coil
LOW	De-energize CB trip coil

Figure 1. Sample PLC control system specification

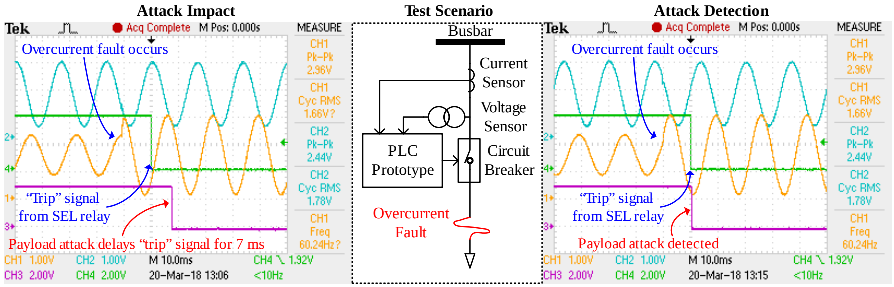
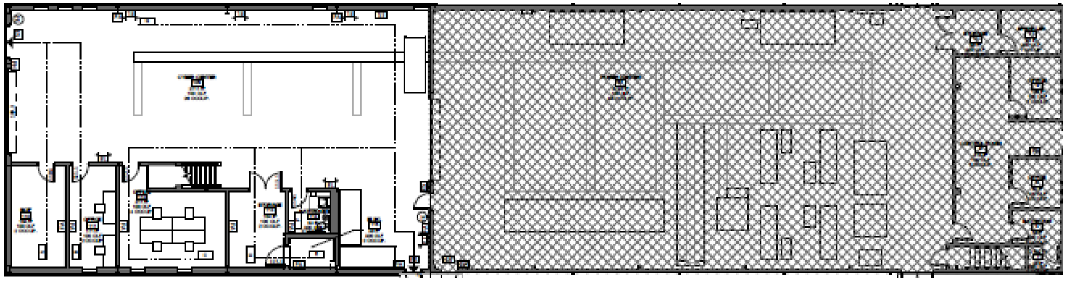


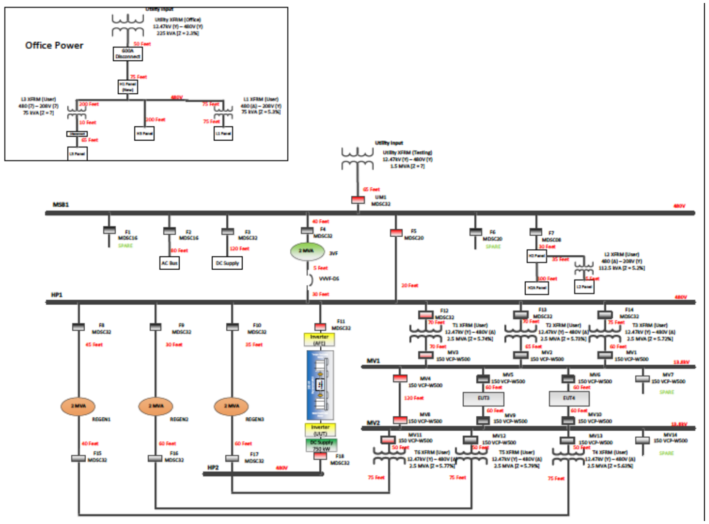
Figure 2. Detection of a "trip" signal delay attack

NCREPT Expansion (UA-Funded)

- **Supporting onsite testing of cybersecurity technologies**
- **Existing Building**
  - 7,000 ft^2
  - 120’ x 50’ + 20’ x 50’ (2nd)

- **Expansion Project Additions**
  - Additional 4,800 ft^2
  - 80’ x 50’ + 12’ x 62’ (2nd)
  - 1500 V / 1500 A dc Bus
  - 480 V / 1200 A ac Bus
  - SCIF (Secret Rating) [400 ft^2]
  - Office space for students/faculty
  - Server/IT room to support Cyber research
  - 120 ton chiller

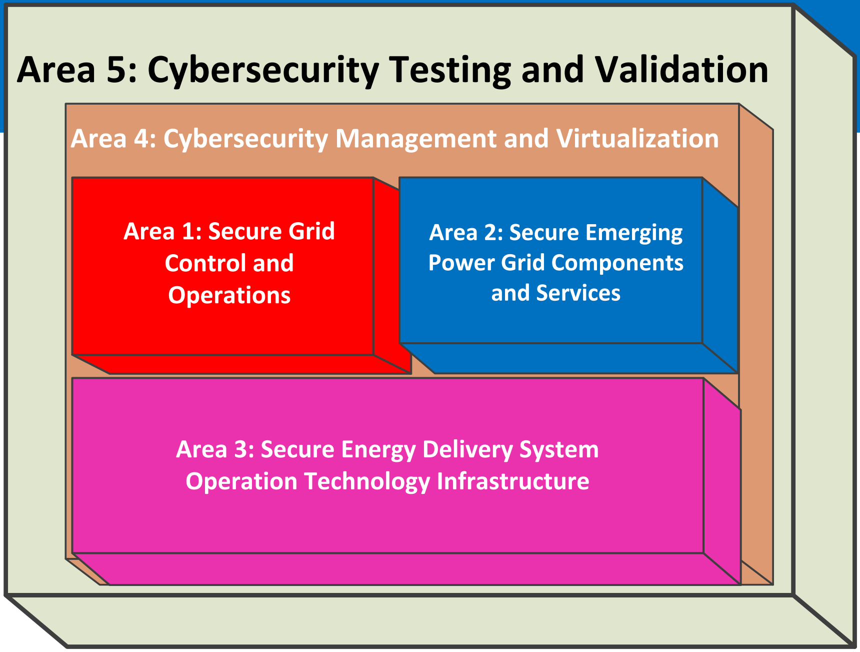




Progress to Date (2/2)

Major Accomplishments

- Automating remediation action analysis for security vulnerabilities
- Detecting compromised devices through system call tracing
- Detecting payload attacks through time-based physical side channels
- Detecting and localizing data falsification attacks in AGC through learning-based and physics-based methods
- Joint detection of data integrity attacks and resilient power state estimation
- Active detection of data integrity attacks
- Detecting and localizing topology attacks through hypothesis testing
- Quickest detection of sparse false data injection attacks
- Detecting unidentifiable false data injection attacks



Area 5: Cybersecurity Testing and Validation
Area 4: Cybersecurity Management and Virtualization
Area 1: Secure Grid Control and Operations
Area 2: Secure Emerging Power Grid Components and Services
Area 3: Secure Energy Delivery System Operation Technology Infrastructure

- Sequence hopping-based fast authentication for IEC 61850 GOOSE messages
- Detecting Botnet in SCADA networks
- Detecting stealthy, low-rate flooding attacks in time-critical communications
- Bloom filter-based public key management for smart meter networks
- Detecting time synchronization attacks against PMU data
- More to come