High-Fidelity, Scalable, Open-Access Cyber Security Testbed for Accelerating Smart Grid Innovations and Deployments

BRUCE WANG, IOWA STATE UNIVERSITY

Cybersecurity Research Acceleration Workshop and Showcase, Indianapolis, IN
October 11, 2017

High-Fidelity, Scalable, Open-Access Cyber Security Testbed for Accelerating Smart Grid Innovations and Deployments

Manimaran Govindarasu

Presented by: Pengyuan (Bruce) Wang

Dept. of Electrical and Computer Engineering

Iowa State University, USA

gmani@iastate.edu
http://powercyber.ece.iastate.edu

NSF Award #: CNS 1446831
Funded by jointly by NSF and DHS

Supported partially by
DOE OE- CEDS grant

Cybersecurity Research Acceleration Workshop and Showcase

October 11, 2017 | Indianapolis, IN

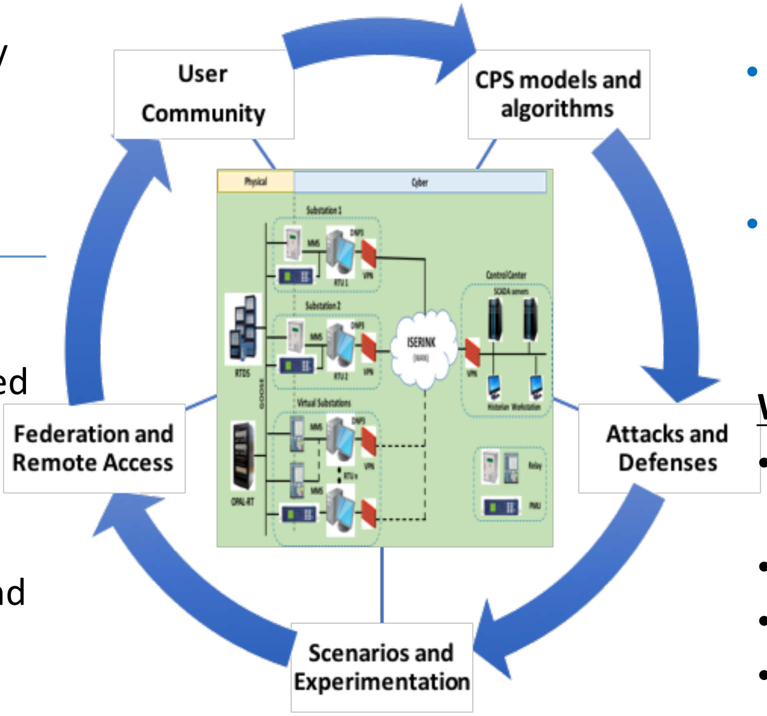
High-Fidelity, Scalable, Open-access Cyber Security Platform for Accelerating Smart Grid Innovations and Deployments

Challenge:

Develop a remotely accessible and cost effective CPS security platform with high-level fidelity and scalability that can serve heterogeneous purposes such as R&D, education, workforce training, etc.

Solution:

- ***High fidelity.*** Build up a HIL testbed that integrates commercial SCADA/EMS system, IEDs and real time power system simulators.
- ***Scalability.*** Apply virtualization and VLAN technologies to improve testbed scalability.
- ***Remote access.*** Develop a web based interface for remote users.
- ***Realistic use cases.*** Replicate realistic cyber attacks and mitigations as study cases.



User Community

CPS models and algorithms

Attacks and Defenses

Scenarios and Experimentation

Federation and Remote Access

NSF CNS #1446831
PI: Manimaran Govindarasu
Team: Douglas Jacobson, Venkataramana Ajjarapu

Value proposition:

- ***TTP.*** Accelerate R&D process and TTP in smart grid.
- ***Education.*** Improve industry workforce's CPS security awareness and skills through effective training.
- ***Collaboration.*** Share resource with remote users and serve as a pilot project of testbed federation.

What we need

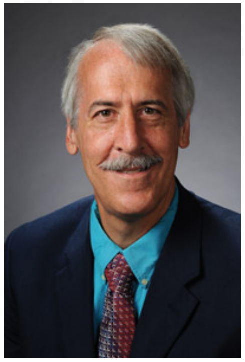
- Industry data sets, real system models and intrusion scenarios
- Academic users for R&D
- Industry users for R&D
- Academic users for education use
- Collaborators for testbed federation

Contact us

Manimaran Govindarasu
Department of Electrical and Computer Engineering,
Iowa State University.
gmani@iastate.edu

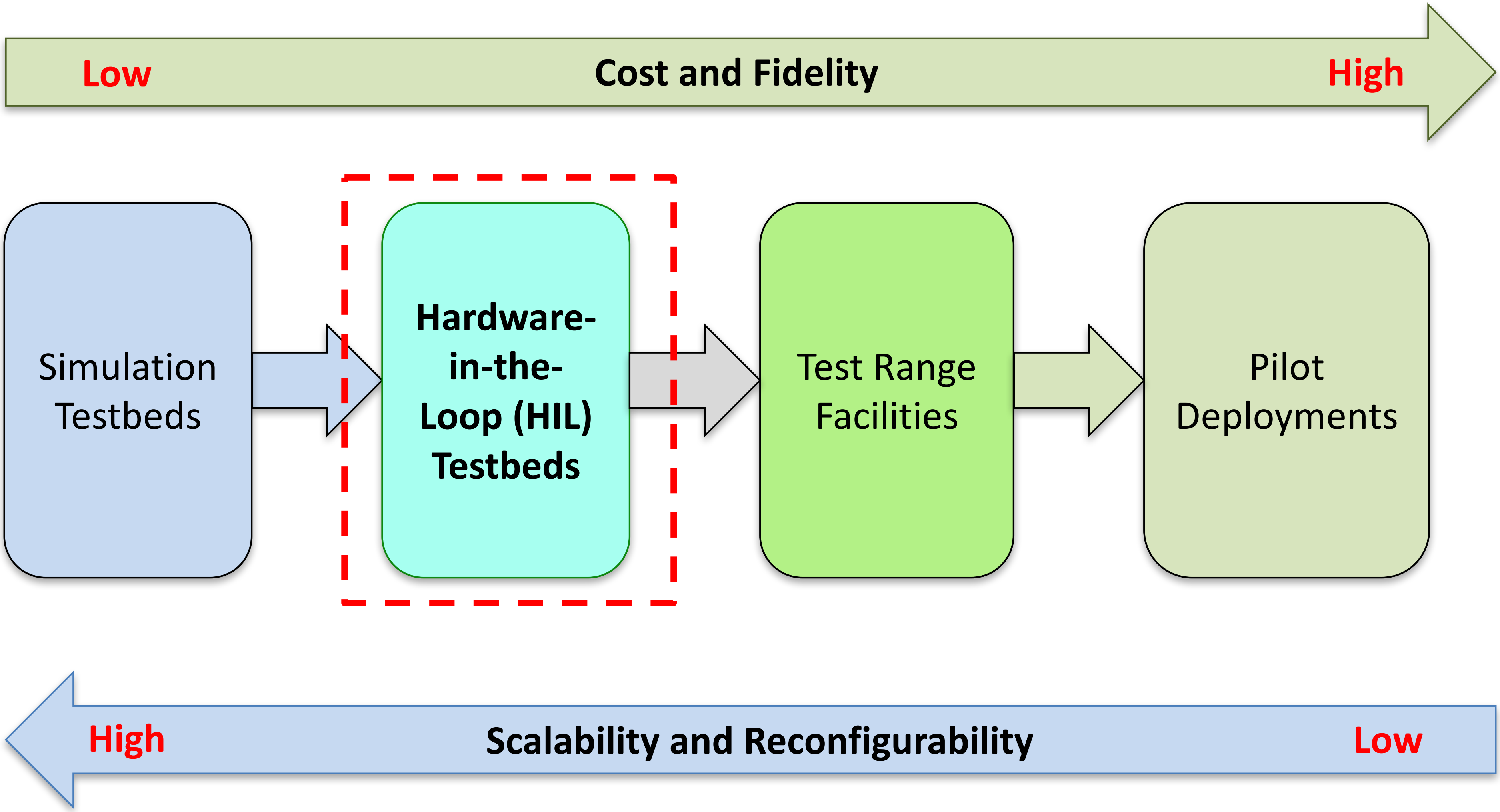
Team Profile

- **Manimaran Govindarasu**, PI
- Douglas Jacobson, Co-PI
- Venkataramana Ajjarapu, Co-PI

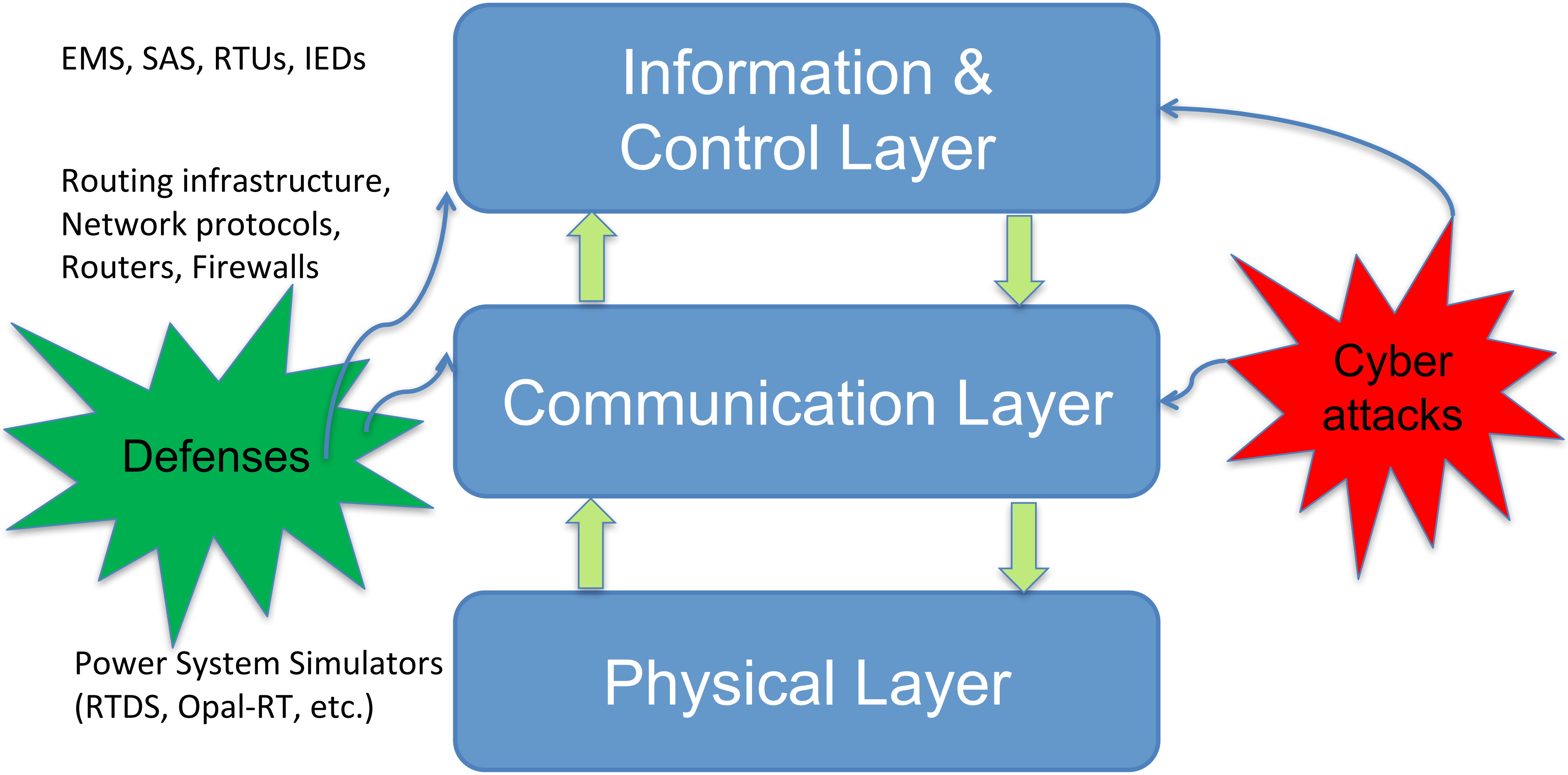


IOWA STATE UNIVERSITY

CPS Security Testbeds



CPS Security Testbed Abstraction



EMS, SAS, RTUs, IEDs

Information & Control Layer

Routing infrastructure,
Network protocols,
Routers, Firewalls

Communication Layer

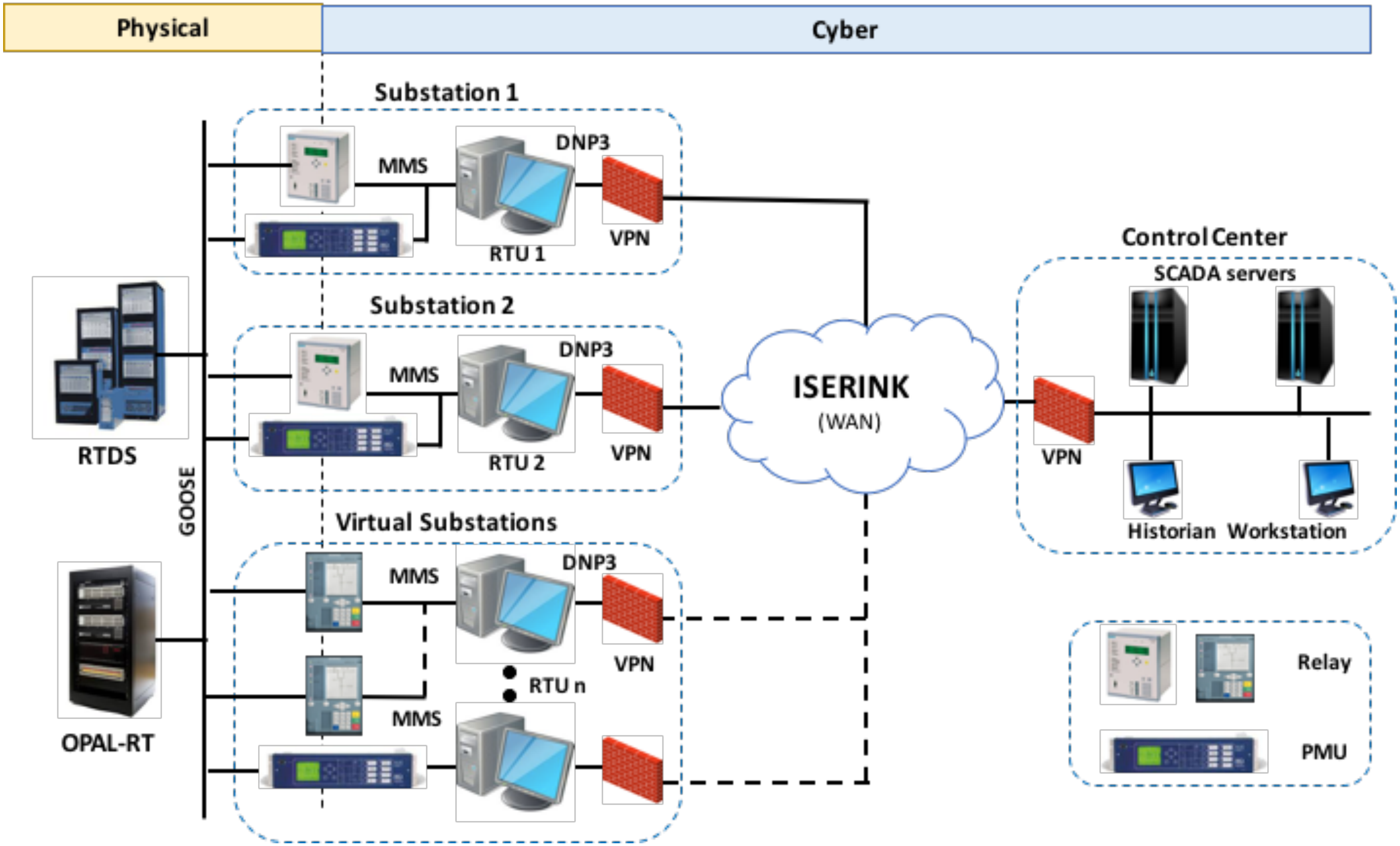
Defenses

Cyber attacks

Power System Simulators
(RTDS, Opal-RT, etc.)

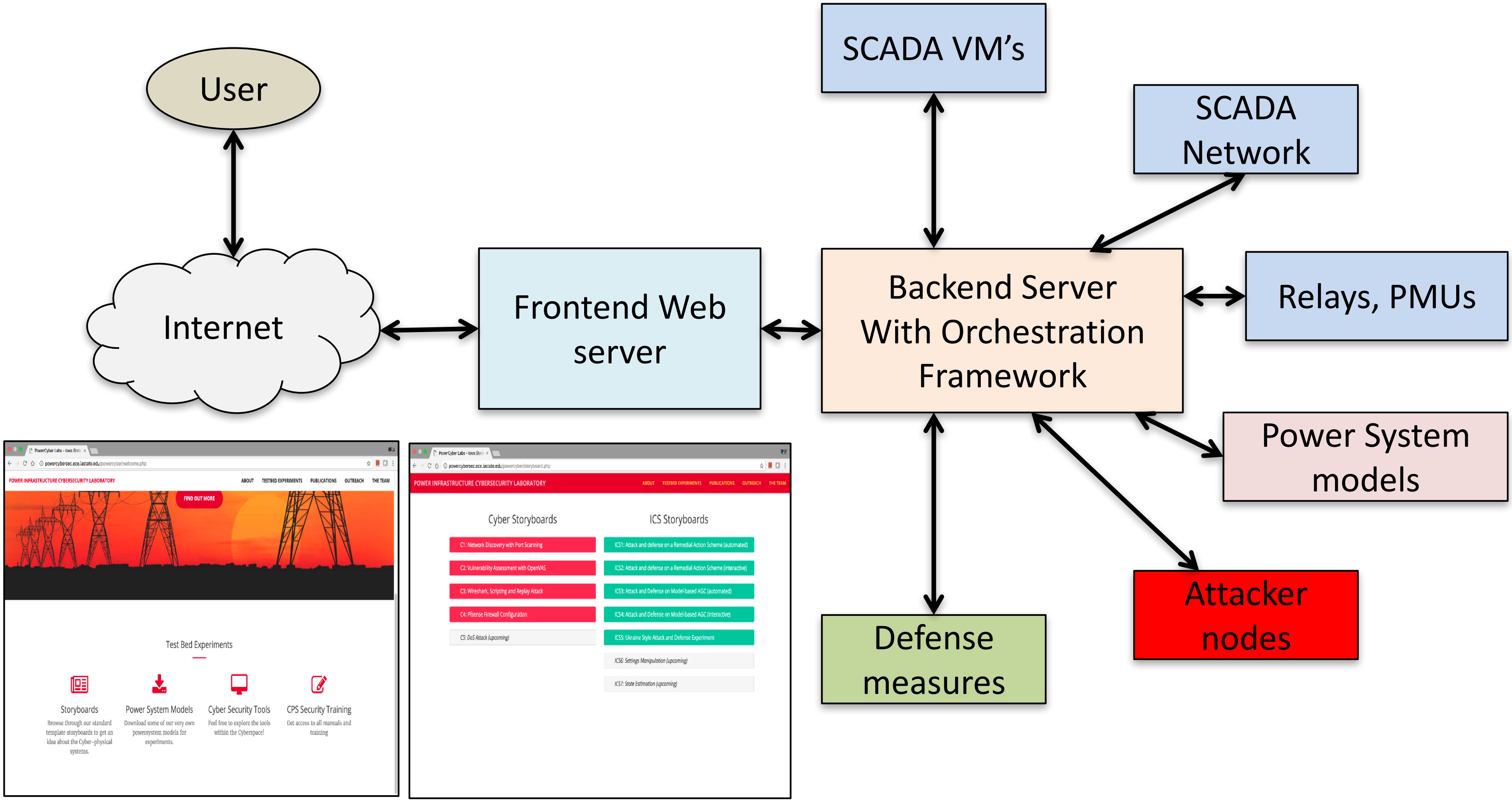
Physical Layer

ISU *PowerCyber* Testbed Architecture



Adam Hahn, Aditya Ashok, Siddharth Sridhar, Manimaran Govindarasu, *Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid,* IEEE Transactions on Smart Grid, vol 4, no. 2, June 2013.

Testbed Remote Access



PowerCyber Labs - Iowa State

powercybersec.ece.iastate.edu/powercyber/welcome.php

POWER INFRASTRUCTURE CYBERSECURITY LABORATORY

ABOUT TESTBED EXPERIMENTS PUBLICATIONS OUTREACH THE TEAM

FIND OUT MORE

Test Bed Experiments

Storyboards

Browse through our standard template storyboards to get an idea about the Cyber-physical systems.

Power System Models

Download some of our very own powersystem models for experiments.

Cyber Security Tools

Feel free to explore the tools within the Cyberspace!

CPS Security Training

Get access to all manuals and training

PowerCyber Labs - Iowa State

powercybersec.ece.iastate.edu/powercyber/storyboard.php

POWER INFRASTRUCTURE CYBERSECURITY LABORATORY

ABOUT TESTBED EXPERIMENTS PUBLICATIONS OUTREACH THE TEAM

Cyber Storyboards

- C1: Network Discovery with Port Scanning
- C2: Vulnerability Assessment with OpenVAS
- C3: Wireshark, Scripting and Replay Attack
- C4: Pfsense Firewall Configuration
- *C5: DoS Attack (upcoming)*

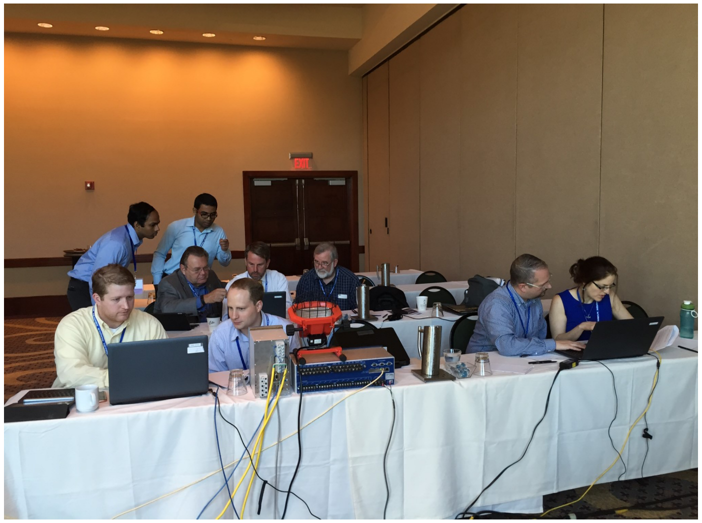
ICS Storyboards

- ICS1: Attack and defense on a Remedial Action Scheme (automated)
- ICS2: Attack and defense on a Remedial Action Scheme (interactive)
- ICS3: Attack and Defense on Model-based AGC (automated)
- ICS4: Attack and Defense on Model-based AGC (interactive)
- ICS5: Ukraine Style Attack and Defense Experiment
- *ICS6: Settings Manipulation (upcoming)*
- *ICS7: State Estimation (upcoming)*

http://powercybersec.ece.iastate.edu

Testbed Users

Symantec	Validating ICS Anomaly-Detection System (ADS).	Research & Development
accenture	Validating Alert Correlation Engine (part of ADS).	
Pacific Northwest National Lab	Validating Attack-Resilient Control (ARC) algorithm for Wide-Area Control.	
Johns Hopkins University	Novel malware detection IPS based on ICMP packets characteristics.	
National Institute of Std. and Tech.	Smart America/ Global Cities Challenge.	
North American Reliability Corporation	Host training for utility professionals in Grid Security Conference .	Training
Electric Power Research Center	Host training for utility professionals in 3 EPRC utilities.	
University of Minnesota, Duluth.	CPS security experiments in EE 533.	Education
Iowa State University	CPS security labs for CprE 539.	
Tokyo Institute of Technology	Exchanging knowledge and experiences of modern HIL testbed	Global cooperation
Black Sea Area Utilities	Demo of typical attacks and discussion on cyber regulation.	



Testbed Users (I)

CLIENT: accenture High performance. Delivered.

Collaborators: Dr. Amin Hassanzadeh, amin.hassanzadeh@accenture.com
Dr. Malek Ben Salem malek.ben.salem@accenture.com

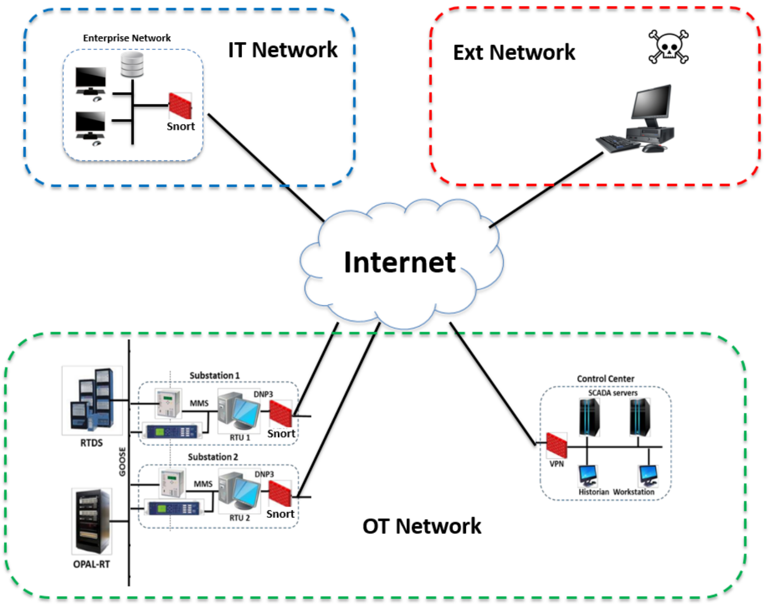
User Goal

- ✓ Validating Alert Correlation Engine (as part of Anomaly Detection System) in a realistic ICS environment.

Approach

- ✓ ICS topology with separate IT, OT and External networks.
- ✓ Realistic attack scenarios that include accessing the OT network through the IT network.
- ✓ ISU team contributed to Accenture's goal in design, implementation, and execution of scenarios.

Deployment Topology



Outcome

Datasets (system logs, firewall logs, IDS logs) that contributed to the design and evaluation of Alert Correlation Engine. Students have gained valuable experience working with industry professionals.

Testbed Users (II)

CLIENT: Pacific Northwest NATIONAL LABORATORY *Proudly Operated by* Battelle *Since 1965*

Collaborators: Dr. David McKinnon, Dr. Siddharth Sridhar, Dr. Aditya Ashok

User Goal

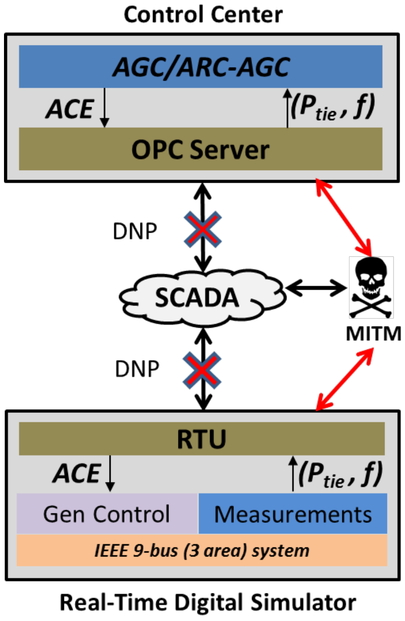
✓ **Validating Attack-Resilient Control (ARC) algorithm for Wide-Area Control on a realistic testbed environment.**

Approach

✓ **Implemented the ARC algorithm on the PowerCyber testbed.**

✓ **Performed realistic cyber attack experimentation involving a typical Man-in-the-Middle attack manipulating AGC measurements.**

Implementation Architecture



- Control center – RTU communication used DNP3 protocol.
- Man-in-the-middle (MITM) attack performed using ARP spoofing.
- Attack modified AGC measurements between control center and RTU.
- Attack injected malicious frequency and tie-line flow measurements based on stealthy attack vectors.

Outcome

✓ **Performance evaluation of ARC on the testbed validated earlier simulation-based studies.**

✓ **Experimental results were published in Resilience Week 2016. Paper awarded ‘Best Paper Award.’**

Testbed Users (III)

CLIENT: NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

COLLABORATOR: **Bill Lawrence**

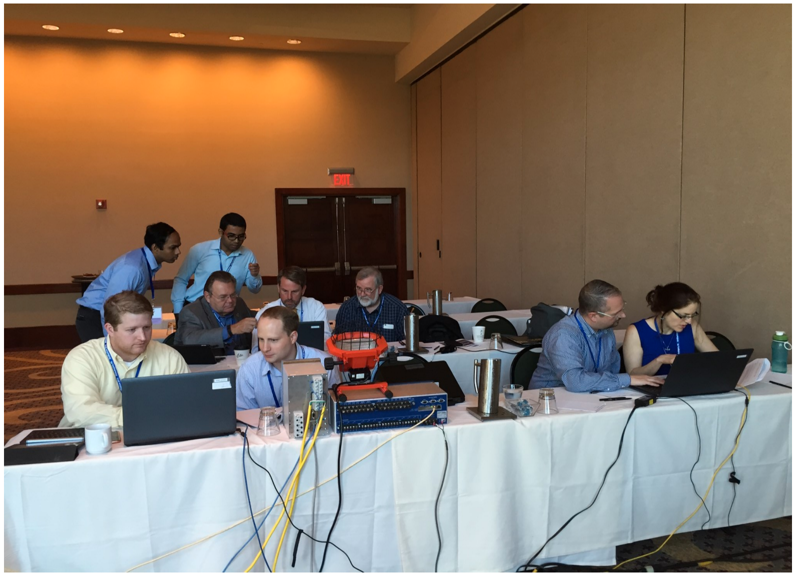
Engagement Goal

Hands on power system cyber-attack and defense via remote access to testbed.

Approach

- ✓ **Module based attack-defense scenarios are developed within a typical SCADA environment.**
- ✓ **Scenarios and task description are provided.**
- ✓ **Provide on-site assistance to help participants go through pre-designed modules.**

During the training



User take-away

- ✓ **Cyber security awareness is highly increased.**

Key Success Factors for TTP

- ***Testbed development*** has been completed smoothly

  - cumulated knowledge over the years

  - interdisciplinary expertise of the team

- ***Multiple use cases*** – R&D, education, training – have been great and created broad impacts

  - understanding of the needs from industry and academia
  - demonstration of the capability of our testbed

- Building ***early users community*** is a success!

  - try to make the cooperation a win-win
  - good communication and coordination is the key

Key Barriers for TTP

- Time and other resources become an issue when more users are supported.

  - Careful resource planning, scheduling, and coordination is critical.

- Insufficiency of models and datasets has become a major obstacle for the researcher to get hands on real problems.

- Sustaining of human resources

  - Mentoring of pipeline of graduate students

Contact Info

Manimaran Govindarasu

Iowa State University
gmani@iastate.edu
515-294-9175
http://powercyber.ece.iastate.edu

Iowa State University

Other Testbed Users

CLIENT: Symantec. Collaborator : **Preeti Agarwal,** preeti_agarwal@symantec.com

User Goal

✓ Validating Symantec ICS Anomaly-Detection System (ADS) in a SCADA environment

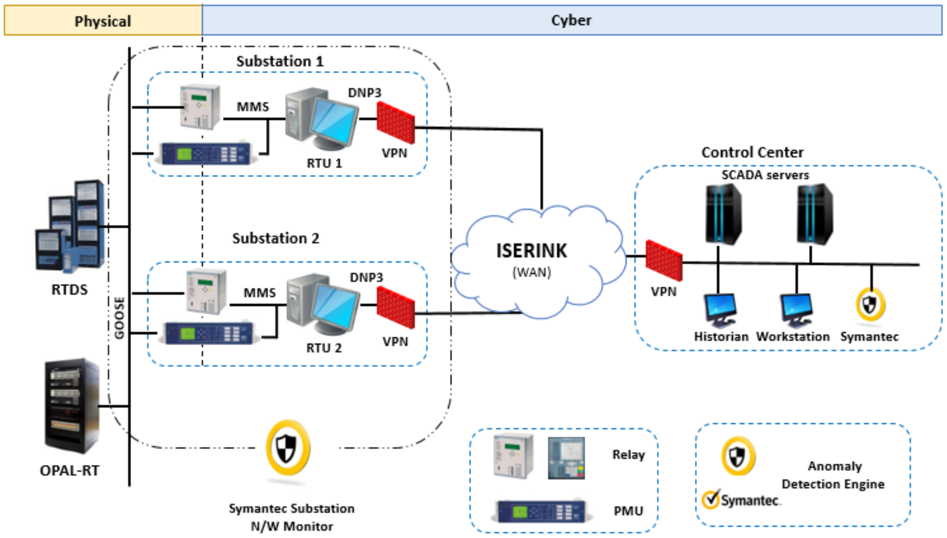
Approach

✓ Integrating Symantec ADS product within ISU's PowerCyber testbed

✓ Executing test-plan by remotely accessing testbed

✓ ISU team to assist Symantec team in testing and evaluation

Deployment Topology



Outcome

✓ ICS-ADS product testing and evaluation results

✓ Trained to profile normal and anomalous SCADA traffic using network traffic monitoring

Other Testbed Users

CLIENT: Johns Hopkins University **Collaborator: Dr. Lanier Watkins,** lanierwatkins@gmail.com

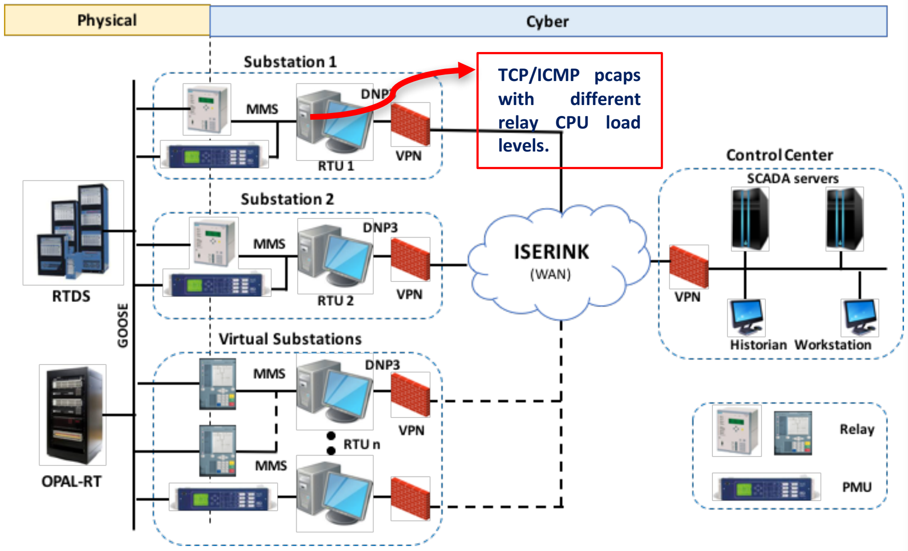
User Goal

- ✓ **Novel IPS design based on PLC ICMP and TCP packet features considering varying CPU load levels.**

Approach

- ✓ **Configure the EMS/SCADA system with specific SIEMENS RTUs and relays located at the substation.**
- ✓ **Configure the relay with CFC charts such that relays can have different CPU usage levels.**
- ✓ **ICMP data collected on the RTU side are delivered as raw data source.**

Deployment Topology



TCP/ICMP pcaps with different relay CPU load levels.

Outcome

Datasets (mainly PLC pcaps captured under different PLC CPU load levels) are delivered and the effectiveness of IPS algorithm has been well verified.

Other Testbed Users

CLIENT: UMD University of Minnesota Duluth Driven to Discover	COLLABORATOR: Dr. Desineni Subbaram Naidu dsnaidu@d.umn.edu
Engagement Goal Experimentation on cyber-attack impact characterization on power grid using remote interface to PowerCyber testbed	**UMD Course** Course: EE5533 Grid: Resiliency, Efficiency & Technology Level: Graduate Background: Electrical Engineering Number of Students: 14
Approach ✓ Presenting an overview about CPS Security for UMN-D Smart Grid class ✓ Introducing Power Cyber testbed with architecture details ✓ Providing overview of Remote access framework with user interface guide	**Lab Assignment** ✓ Experimenting cyber attack impact characterization – quantify power flow, voltage, frequency ✓ Performing cyber-attacks on different power system models – a Wide Area Protection Scheme ✓ Experimenting different types of attacks on each model – Coordinated attacks (DoS, data integrity)
Students Learning ✓ Identifying most impactful cyber attack by comparing pre & post attack values on power system.	

Other Testbed Users

CLIENT: **Black Sea Utility Regulators from Ukraine, Georgia, etc.**

COLLABORATOR: **Paul Sinton Stack** pstack@narus.org

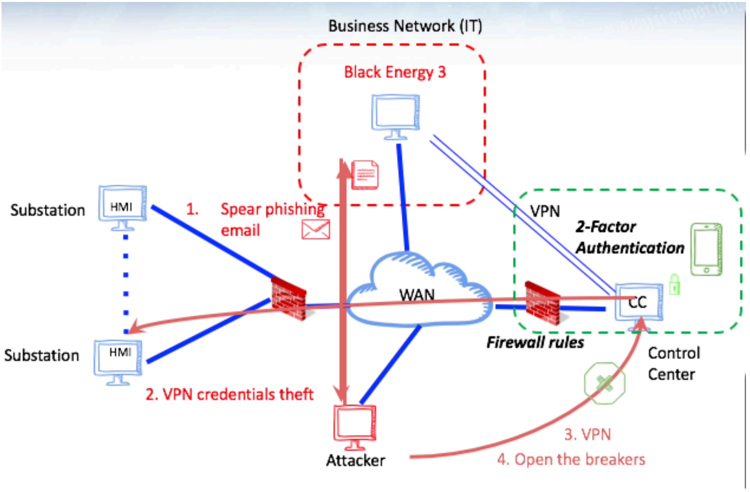
Engagement Goal

Demonstration & comprehensive analyses of 2015 Ukrainian Attack and effective mitigation, utility policy and regulation.

Approach

- ✓ **Demonstration of Ukrainian attack**
- ✓ **Demonstration of other power system attack scenarios**
- ✓ **Discussion among utilities, researchers and regulators.**

Ukrainian Attack Implementation



Visitor Learning

- ✓ **Learning about the best practices to make power system secure and the proper procedures to carry out of relevant regulation and implementation.**

Other Testbed Users

CLIENT: **Cedar Falls Utilities**
Central Iowa Power Cooperative
MidAmerican Energy

COLLABORATOR: **Josh Hoppes** Josh.Hoppes@cfunet.net
Chad Miller Chad.miller@cipco.net
Patrick Ryan pkryan@midamerican.com

Engagement Goal

Hands on power system cyber-attack and defense via remote access to testbed.

Approach

- ✓ **Module based attack-defense scenarios are developed within a typical SCADA environment.**
- ✓ **Scenarios and task description are provided.**
- ✓ **Provide on-site assistance to help participants go through pre-designed modules.**

Training Assignment

Module 1: Reconnaissance as an attacker.
Active hosts and services discovery with NMAP

Module 2: Vulnerability analysis tool application.
Application of OpenVAS

Module 3: Cause power loss with replay attack.
Packets sniffing with wireshark, and python script coding to trip circuit breakers.

Module 4: Best defense practice.
Apply host firewalls, network egress filtering as mitigation.

User Learning

- ✓ **Understanding how cyber attack can take place step by step in power system and learning about proper mitigations.**

Survey Tools to Collect Feedback

Workshop Overall:

http://bit.ly/ttpindyws

Researcher Assets:

http://bit.ly/ttpindyresearch