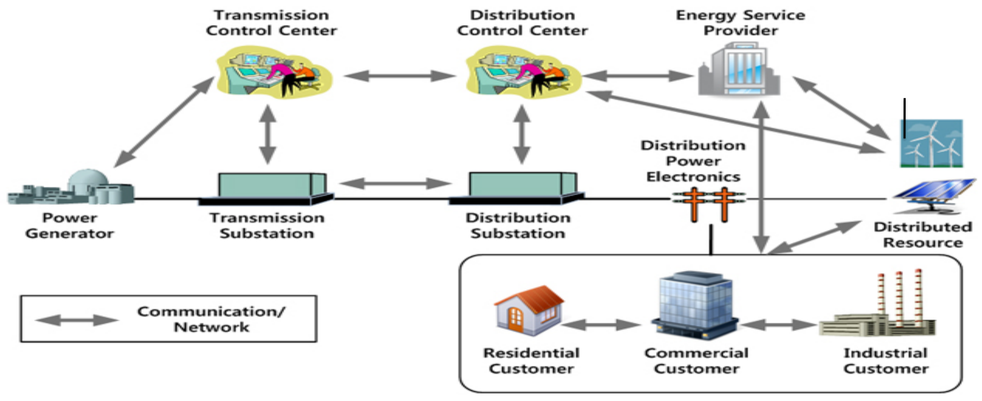
PowerCyber – A CPS Security Testbed for Secure and Resilient Smart Grid

Aditya Ashok, Manimaran Govindarasu

PowerCyber Laboratory, Department of Electrical and Computer Engineering, Iowa State University.

aashok@iastate.edu, gmani@iastate.edu

• Smart Grid – A Cyber Physical System



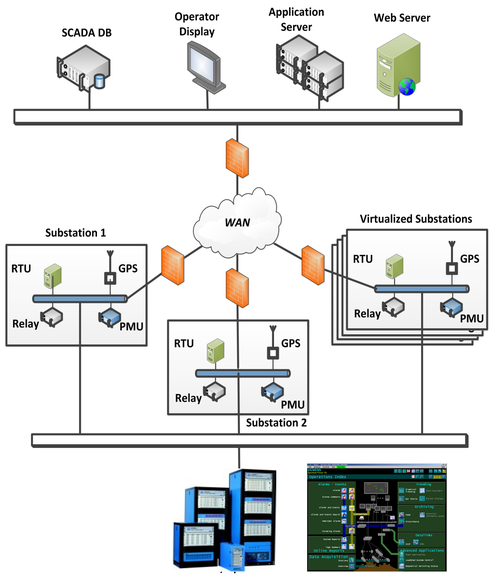
- Smart grid increases dependence on high-speed, automatic, monitoring and control technologies.
- Adversaries can act through the cyber infrastructure to inflict damage on the planning, operations and market functions of the power grid.
- Cyber attacks on critical infrastructures are increasing in number and sophistication (e.g. Stuxnet).
- Several standards and roadmaps have been put out for ensuring Cyber security compliance in Smart Grid: NERC CIP, NISTIR 7628, DoE 2011 Roadmap to Achieve Energy Delivery Systems Cyber security.

• PowerCyber CPS Testbed – Salient Features

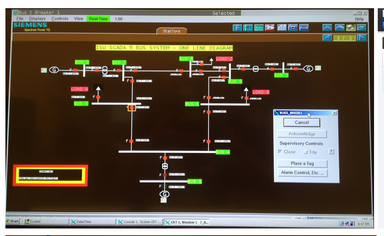
1. Cyber-in-the-Loop Real-Time Simulation *environment modeling bulk power system*

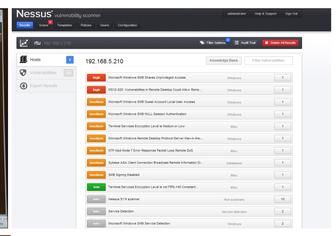
2. Scalability:
- RTDS/Opal-RT provide ability to simulate large power systems with control and protection functions in real-time.
- Multi-area, substation architecture enabled through virtualization.

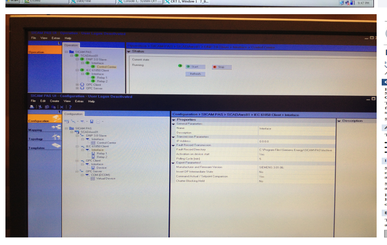
3. High Fidelity:
- Industry-grade SCADA/EMS and substation automation
- WAN emulated using ISEAGE; DNP3 and IEC61850 protocols used for SCADA;
- Industry-grade security appliances for VPN/firewall.
- Local/wide-area control and protection applications emulated with programmable IED and PMU interfaced with RTDS/Opal-RT.



4. Remote Access: Web-based access for remote experimentation with custom power/cyber system models and attack templates.





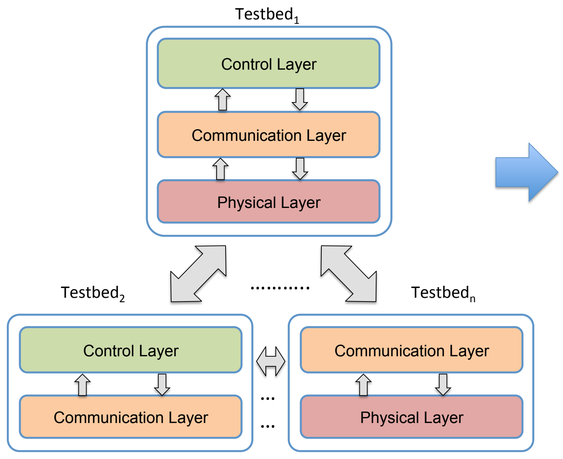


Capabilities

- Vulnerability Assessment
- Attack-Defense Evaluations
- System Impact Analysis
- Security Product Testing
- Risk Assessment
- Education
- Risk Mitigation Studies
- Industry Short-Courses

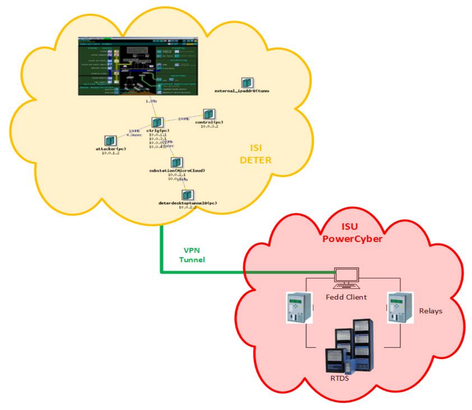
• Energy CPS Testbed Federation

Federation architecture



Implementation

Smart Energy CPS
ISU PowerCyber + ISI DeterLab



• Demo @ Smart America Challenge

Smart America Challenge Vision: Demonstrate the benefits of interconnected Cyber-Physical Systems including improved safety, sustainability, efficiency, healthcare, and travel.

Scenario execution

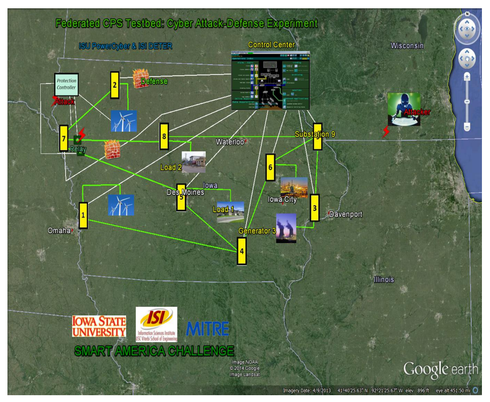
Federation setup (ISU and DETER)
- **SCADA Control Center** and **Energy Management Systems** (EMS) running inside DETER.
- **Substation Automation Systems** (SAS) running inside both DETER and ISU PowerCyber.
- Physical **relays** and **Real-Time Digital Simulator** (RTDS) running in ISU PowerCyber.

Coordinated attack (ISU and DETER)
- **Data integrity attack** from ISU PowerCyber
- **DoS attack** from DETER

Defense capabilities (ISU and DETER)
- **IDS/IPS** for Packet dropping @ Substations
- **Traffic filtering** @ Substations

Visualization (ISU)
- **OPC server** interface with SICAM
- **Google earth** interface

Visualization



Team

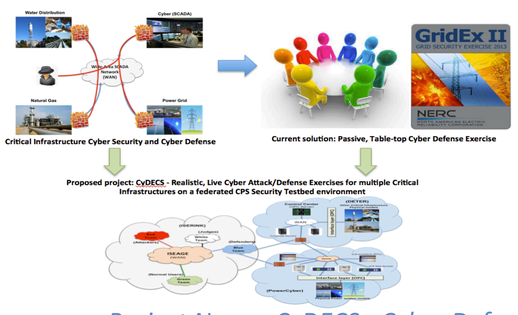
IOWA STATE UNIVERSITY OF SCIENCE AND TECHNOLOGY
MITRE
NATIONAL INSTRUMENTS
NREL
NC STATE UNIVERSITY
PENNSTATE
Scitor Corporation
THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL
USC Viterbi School of Engineering

Demo (June 11, 2014 @ Washington, D.C.) link: http://powercyber.ece.iastate.edu/SmartAmerica_Demo.mp4

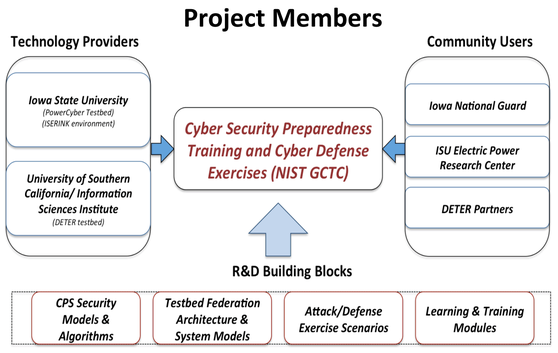
• NIST/US Ignite Global City Teams Challenge

Global City Teams Challenge Vision: Create a platform for communities and innovators to create teams that will foster the spread of "smart cities" that leverage networked technologies to improve resource utilization, efficiency, security and quality of life.

Motivation



Project Members

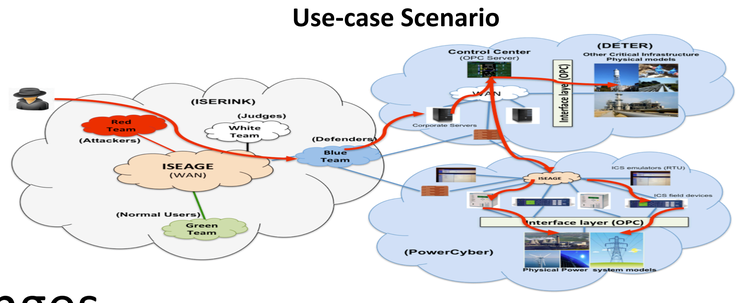


Project Name: CyDECS - Cyber Defense Exercises for Critical Infrastructure Cyber Security

Project Goal: *Develop and deploy an integrated environment to conduct security planning, risk assessment, attack-defense training and education for the community, government and industry stakeholders.*

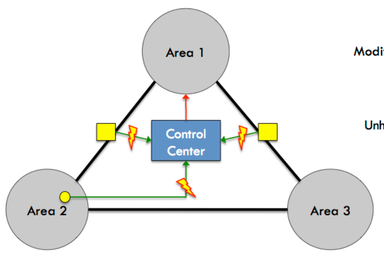
- *Demo @ Global City Teams Festival in June 2015.*

Use-case Scenario



• Cyber Attack/Defense Experimentation

Coordinated attacks on Wide-Area Control (Automatic Generation Control)*^



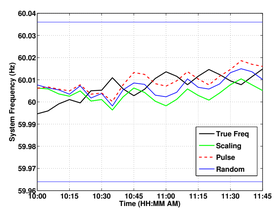
Attack

Modify tie-line flow and frequency measurements

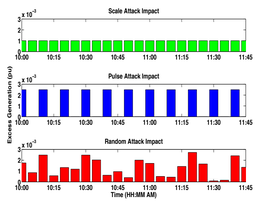
Impact

Unhealthy operating frequency conditions

Impact: System Frequency



Impact: Excess Generation

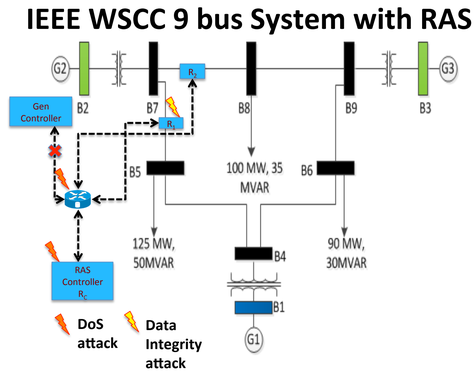


- We have implemented a three area AGC scheme on the WECC 9 bus system.
- **Coordinated attack vector –** Manipulate frequency and multiple tie-line measurements consistently to impact system frequency. The attack types are scaling, pulse and random data integrity attacks.

Coordinated attacks on Wide-Area Protection (Remedial Action Schemes (RAS))**

- Adapted a protection scheme from WECC RAS list on the WECC 9 bus system.
  - **RAS details**: Reduce generation if one of the two lines to which it is connected to has a fault, provided that the generation is above a threshold
- **Coordinated attack vector**
  - Creating a Data Integrity attack to trip the Relay 1 which protects line 7–5 to activate the RAS.
  - Creating a Denial of Service attack to prevent the GOOSE trip command to the generation unit at bus 2 to result in a thermal overload on line 7 – 8 and cause it to trip out.

IEEE WSCC 9 bus System with RAS



• Research Challenges

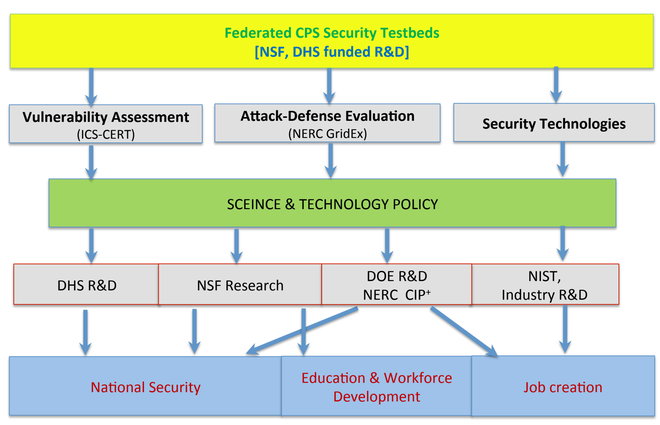
Security and Resiliency

1. Fundamental paradigm to **transform "fault-resilient grid of today into an attack-resilient grid of the future"** taking into account both natural and man-made extreme events.
2. Pragmatic **risk modeling and mitigation framework** accounting evolving, uncertain nature of threats (APTs and HILFs), cyber-physical interdependencies, and cascading failures.
3. **Security architectures and algorithms** to achieve security, privacy, and resiliency in wide-area monitoring, protection, and control of the power grid.

Federated CPS Infrastructures & Testbeds

1. Development of a **national-scale high-fidelity, federated CPS testbed** – with remote and open access – to accelerate the pace of innovation, R&D, education, and workforce development
2. **CPS Cloud architecture, algorithms, and services** for resource allocation and control of federated resources to support large-scale, high-fidelity CPS experimentations
3. A open and shared **experimental infrastructure for cross cutting CPS sectors** (e.g., power system, oil and natural gas, transportation)

• Broader Impacts



*Siddharth Sridhar, Manimaran Govindarasu, Model-based Attack Detection and Mitigation for Automatic Generation Control, IEEE Transactions on Smart Grid, Vol. 5, N0. 2, March 2014.
^ Aditya Ashok, Pengyuan Wang, Matthew Brown, Manimaran Govindarasu, Experimental Evaluation of Cyber Attacks on Automatic Generation Control using a CPS Security Testbed, To appear in Proceedings of IEEE PES GM 2015.
**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, Issue 2, 2013.

IOWA STATE UNIVERSITY
Department of Electrical and Computer Engineering

Acknowledgements: This work is funded by National Science Foundation grants CNS 0915945, CNS 1329915, ECCS 1202542. We would also like to acknowledge the support of Iowa State Electric Power Research Center for the research.