Research goal:

Transform “fault-resilient grid” of today to an “attack-resilient grid” of the future

CPS Security Testbed for Smart Grid

Manimaran Govindarasu

Iowa State University

Email: gmani@iastate.edu

Web: http://powercyber.ece.iastate.edu

JST-NSF-DFG-RCN Workshop on Distributed Energy Management Systems

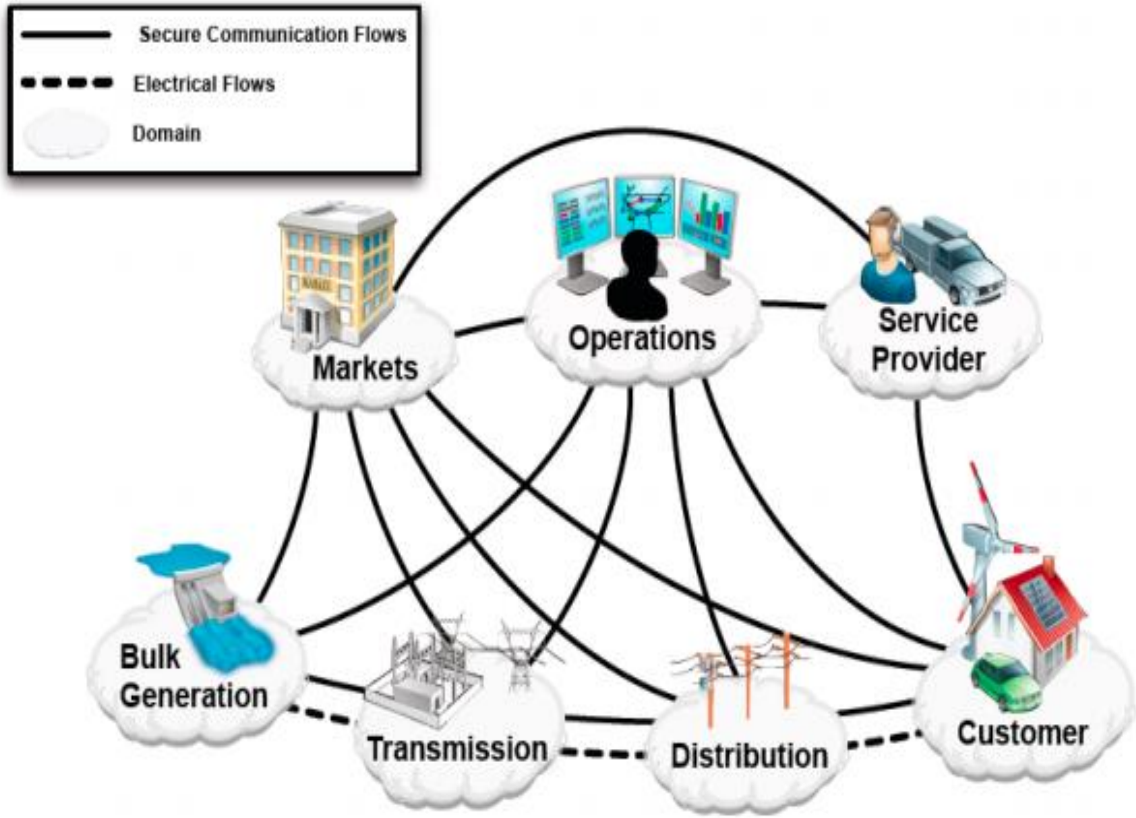
This research is funded by NSF CPS, ECCS, and SaTC programs

Part of this research done in Collaboration with
Dr. Chen-Ching Liu, Washington State University

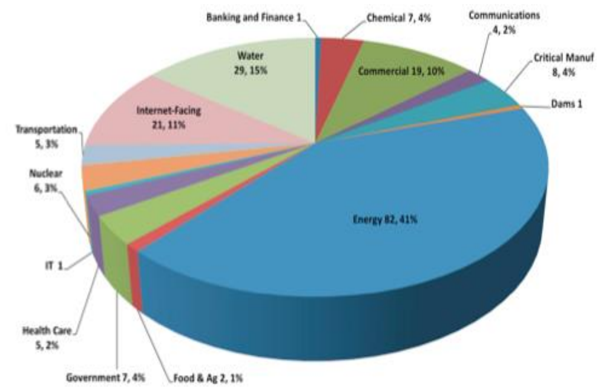
Outline

- Motivation for CPS Security Experimentation
- Science of Experimentation
- Engineering CPS Testbed
- ISU *Powercyber* Security Testbed
- Testbed Federation & Case Studies
- Conclusion & Future work

Smart Grid: A Cyber-Physical System



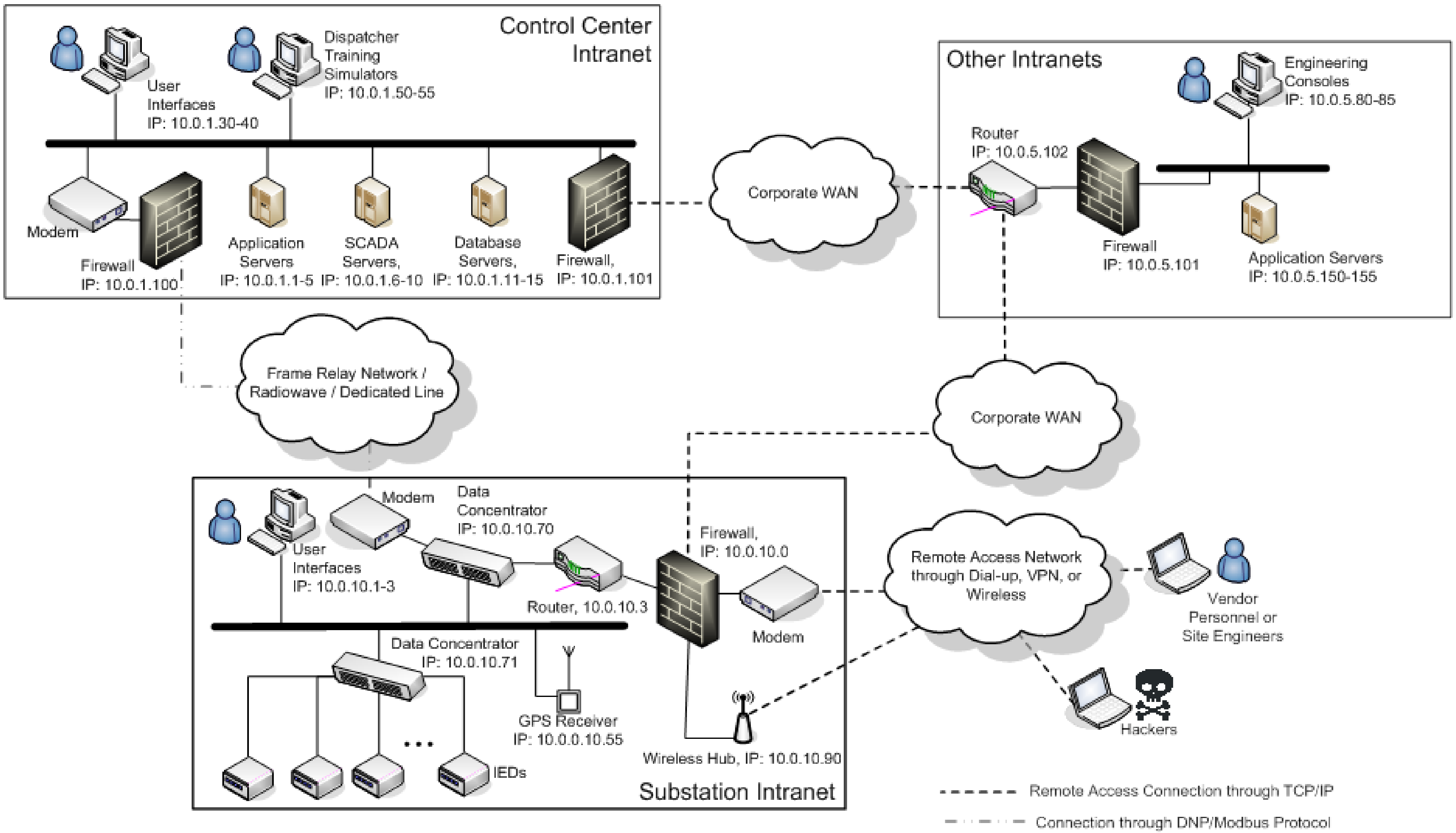
DHS ICS-CERT Cyber incident Report (2012)



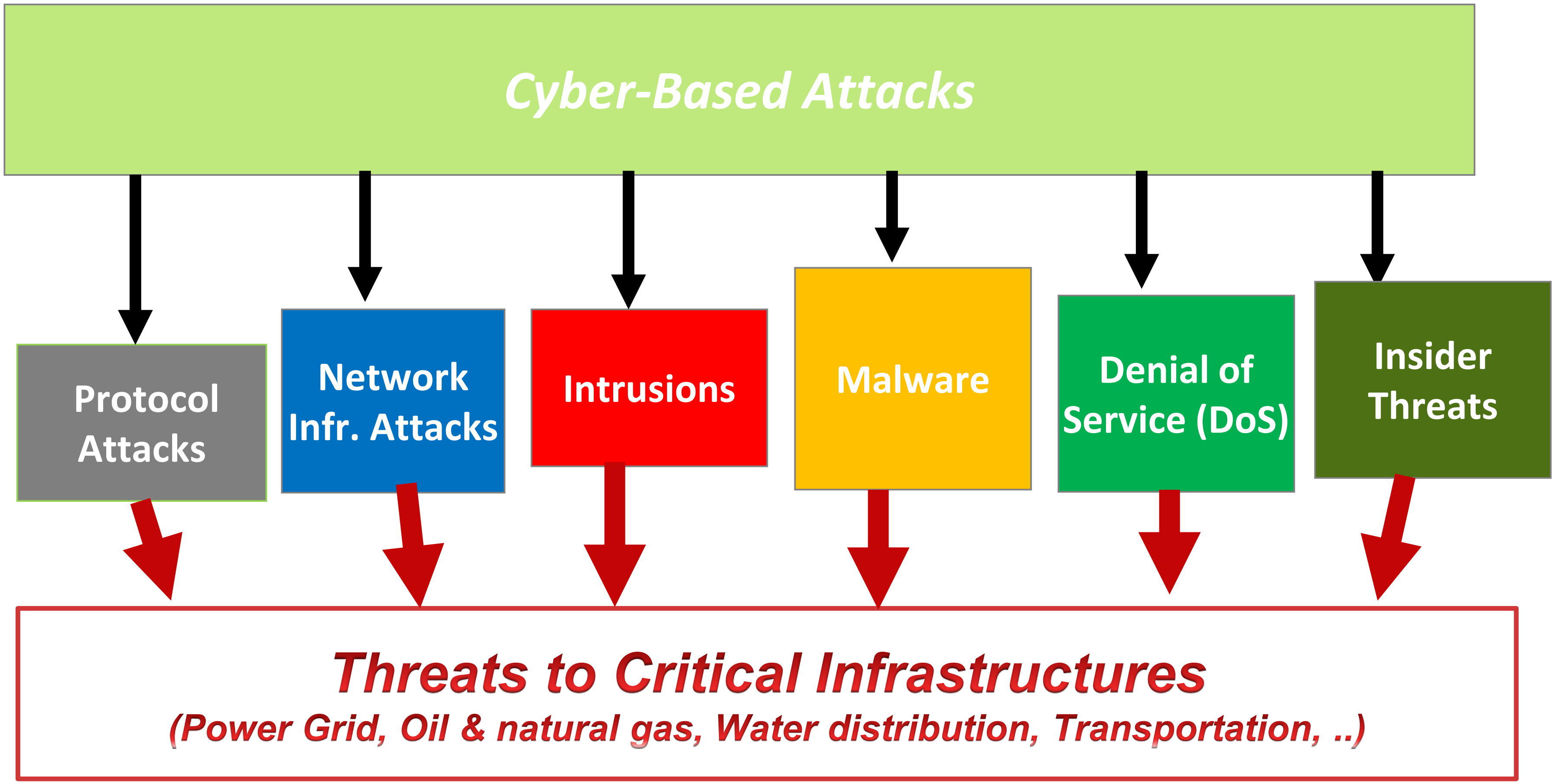
Energy infrastructure: 41% (82)

Source: **NIST Framework and Roadmap for Smart Grid Interoperability Standards (Feb. 2012)**

Power grid control network

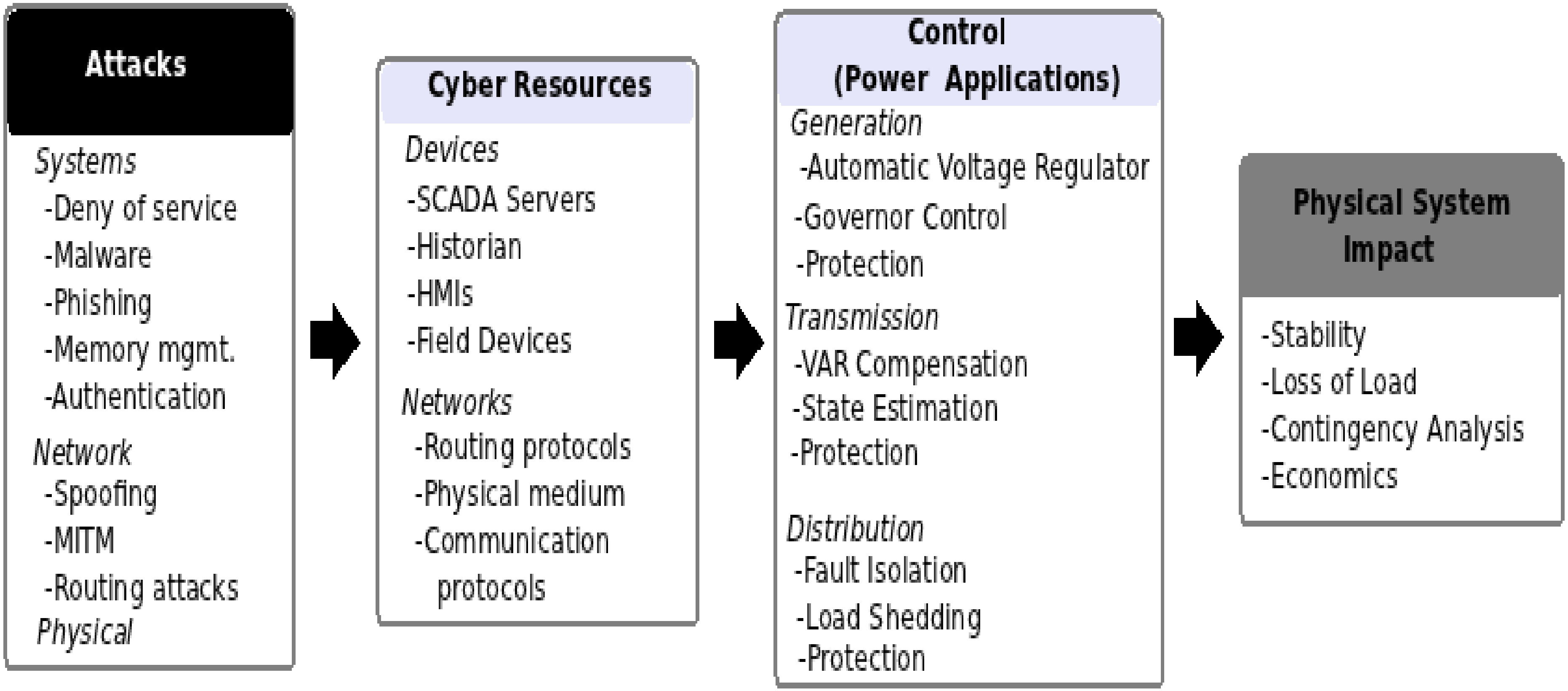


Cyber Threats to Critical Infrastructures



[**General Accounting Office, CIP Reports, 2004 to 2010**]; [NSA "Perfect Citizen", 2010]:
Recognizes that critical infrastructures are vulnerable to cyber attacks from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and other malicious intruders.

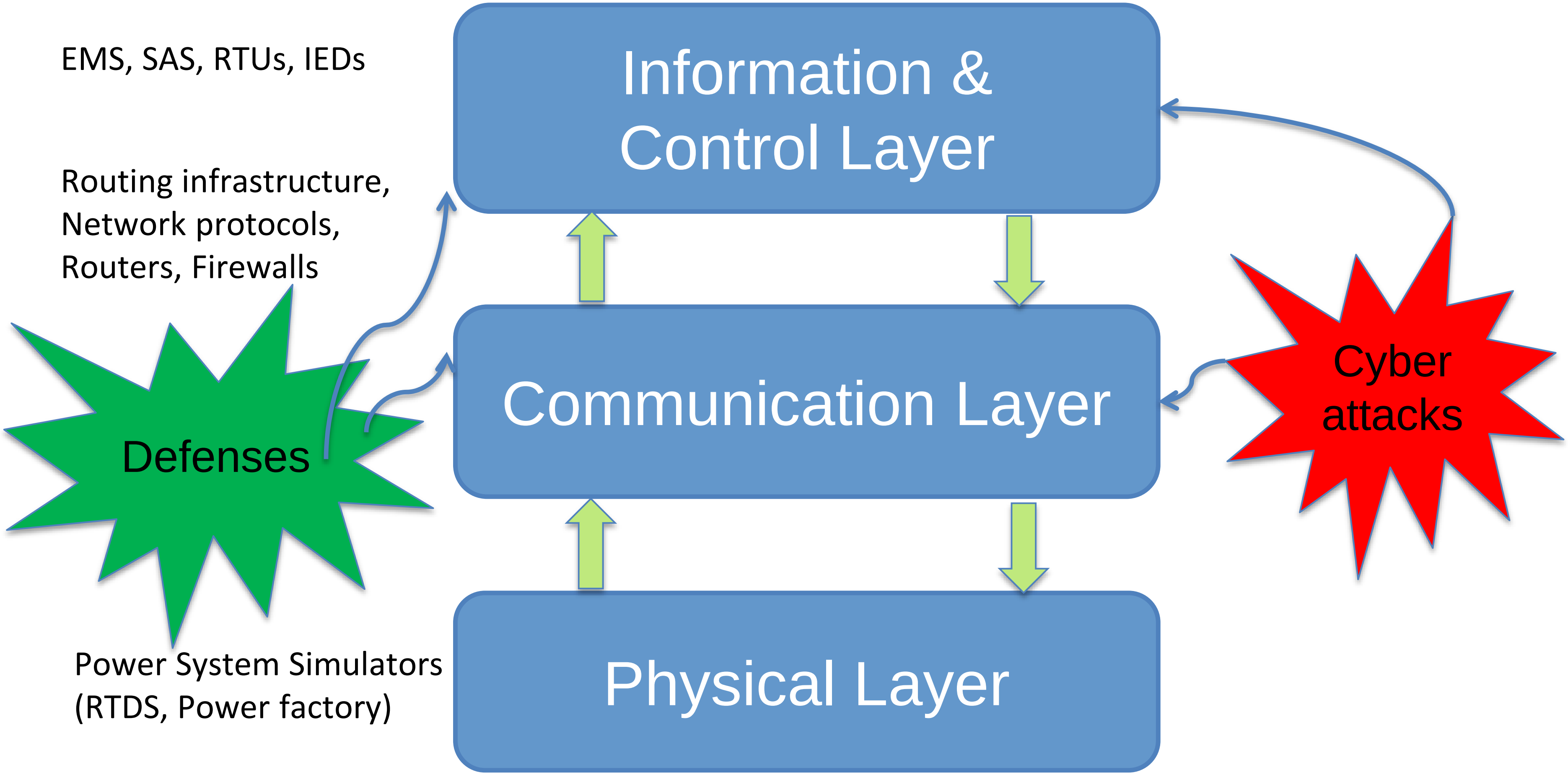
Attacks-Cyber-Control-Physical



Testbed Definition

- "A **testbed** is a platform for conducting rigorous, transparent, and replicable testing of scientific theories, computational tools, and new technologies." - *Wikipedia*

CPS Testbed – A Layered View



Motivation for Testbeds & Design Tradeoffs

Realistic platform for model validation

- Power system dynamics
- Communication systems dynamics
- Control applications

Realistic platform for experimental evaluation

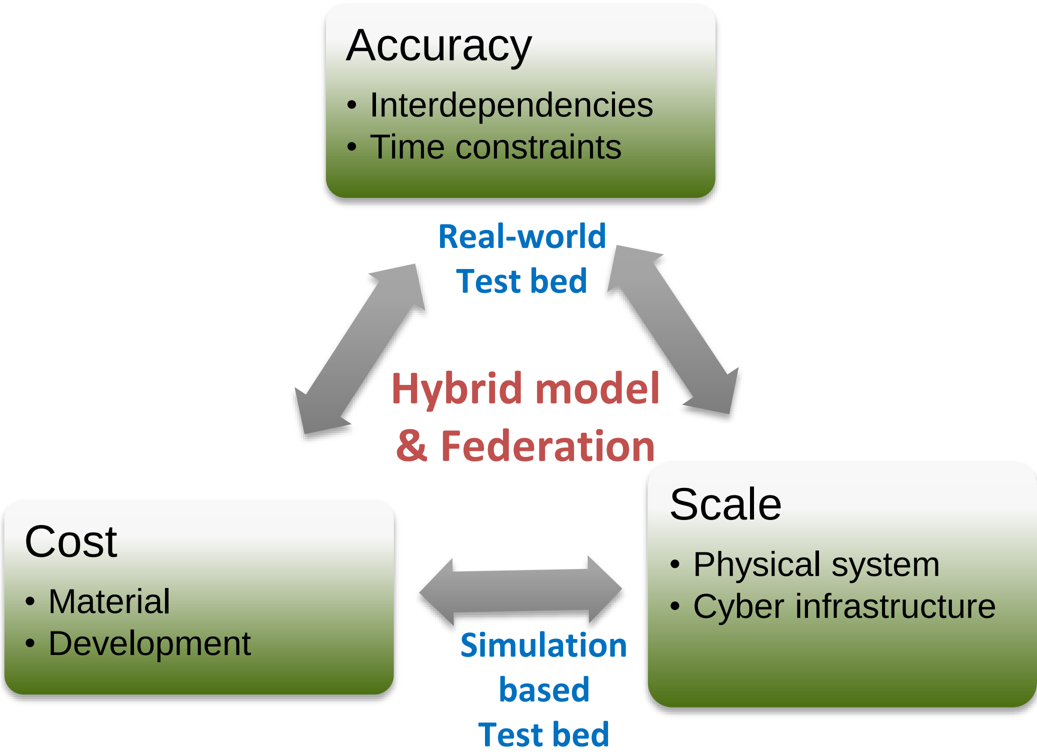
- Cyber-Control-Physical interactions
- Evaluation of CPS architectures, models, and algorithms

Accelerate Innovation

- Accuracy, Programmability, Repeatability

Bridge Theory and Practice

Pathway from Academic Research to Industry Practice

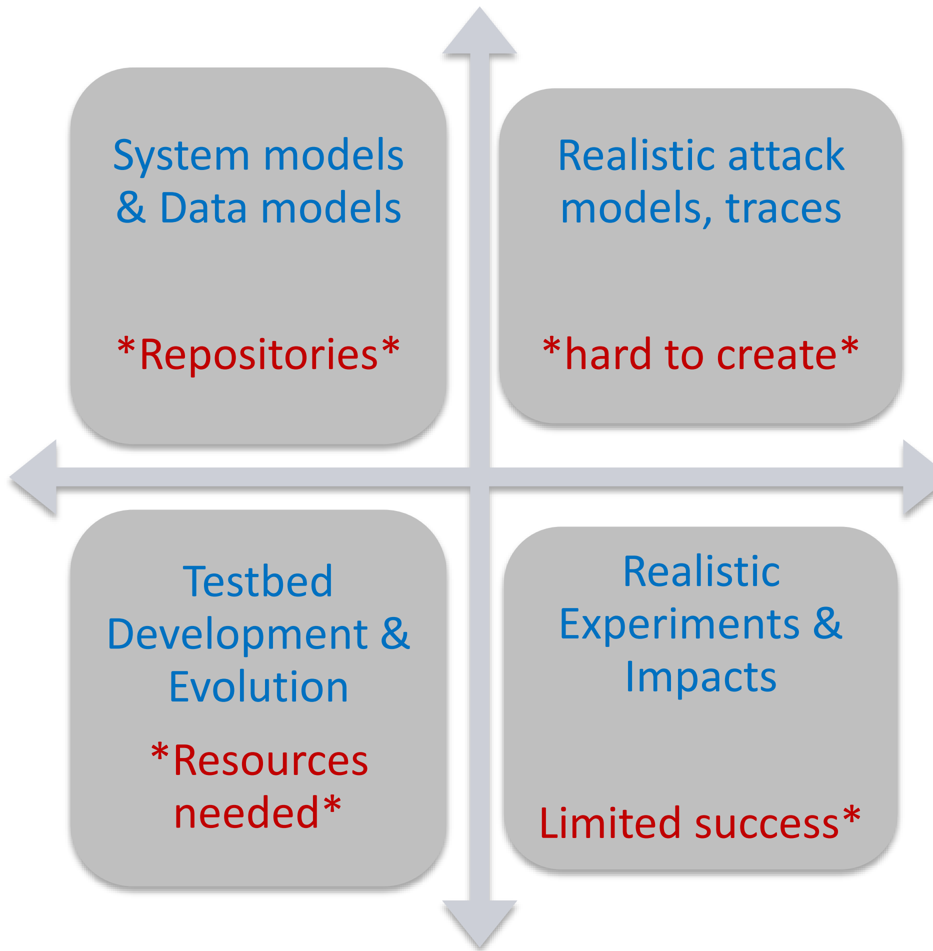


Science of Experimentation

- Time Sync – cyber and physical worlds
- Virtual time or Real-time?
- Fidelity – what level?
- Abstractions & Modularity – right level?
- Scalability – both cyber and physical
- Representativeness – how realistic?
- Repeatability & reproducibility of results

Engineering the Testbed

- Cyber-Physical integration
- Hardware-in-the-loop
- Cyber-in-the-loop
- Re-configurability
- Interoperability
- Federation
- Standard models, datasets
- Open, Remote access?



Testbed R&D Applications

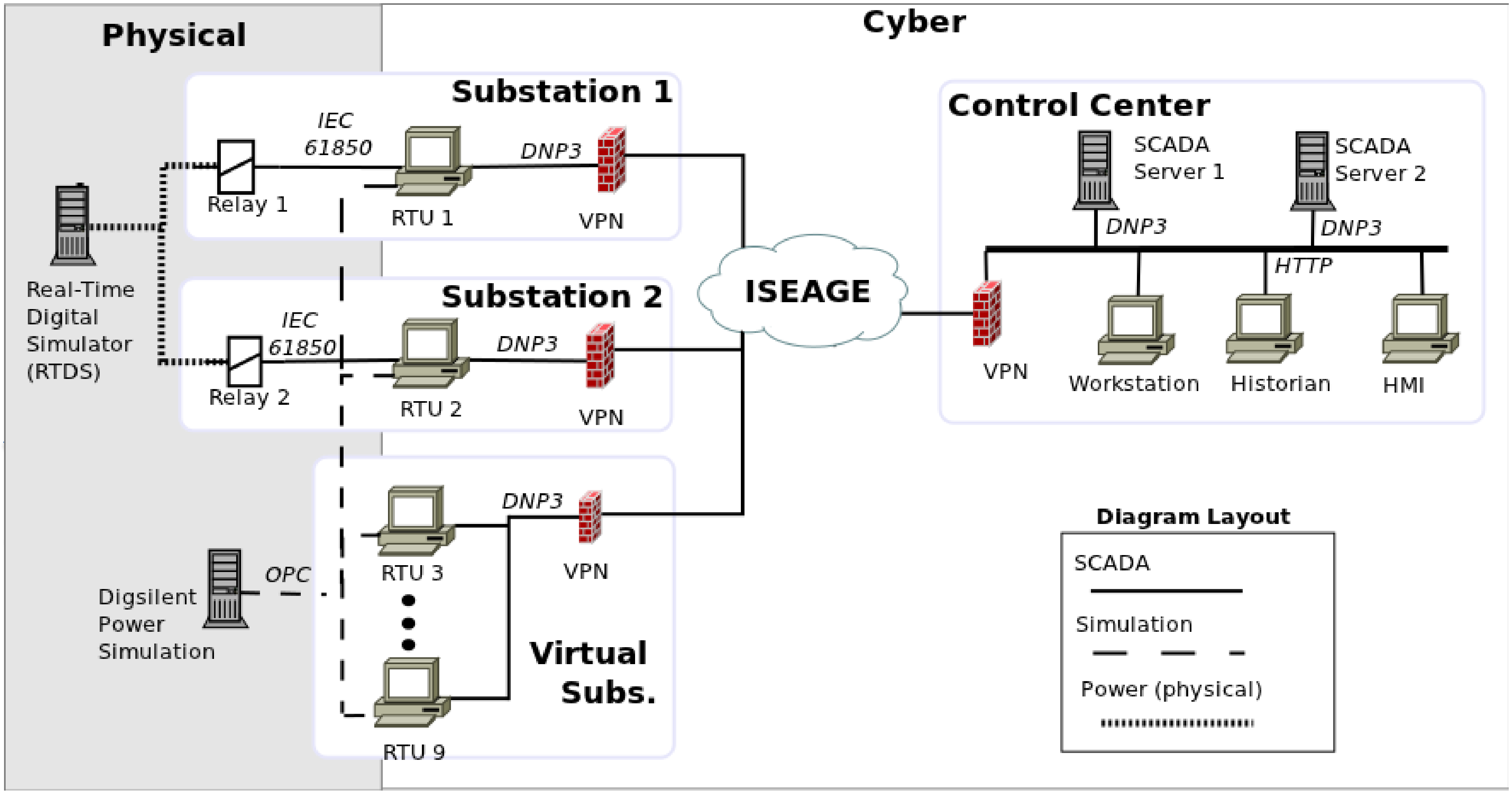
1. Vulnerability Analysis
2. Impact Analysis
3. Mitigation Research
4. Cyber-Physical Metrics
5. Data and Model Development
6. Security Validation
7. Interoperability
8. Cyber Forensics
9. Operator Training

Cyber Security Testbeds for Smart Grid

- National SCADA test bed (NSTB) @ Idaho National Lab
- Virtual Control System Environment @ Sandia National Lab
- SCADA Security Testbed @ Pacific Northwest National Lab
- **PowerCyber Security Testbed @ Iowa State University**
- SCADA Security Testbed @ Washington State University & UC Dublin
- Virtual Power System test bed (VPST) @ University of Illinois, Urbana-Champaign
- Critical Infrastructure Security Testbed @ Mississippi State University
- Smart Grid in a Room @ CMU
- A few Testbeds in Europe – VIKING project, CRUTIAL project

ISU *PowerCyber:* CPS Security Testbed

- an unique platform for experimental R&D



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.

ISU *PowerCyber* Testbed - Features

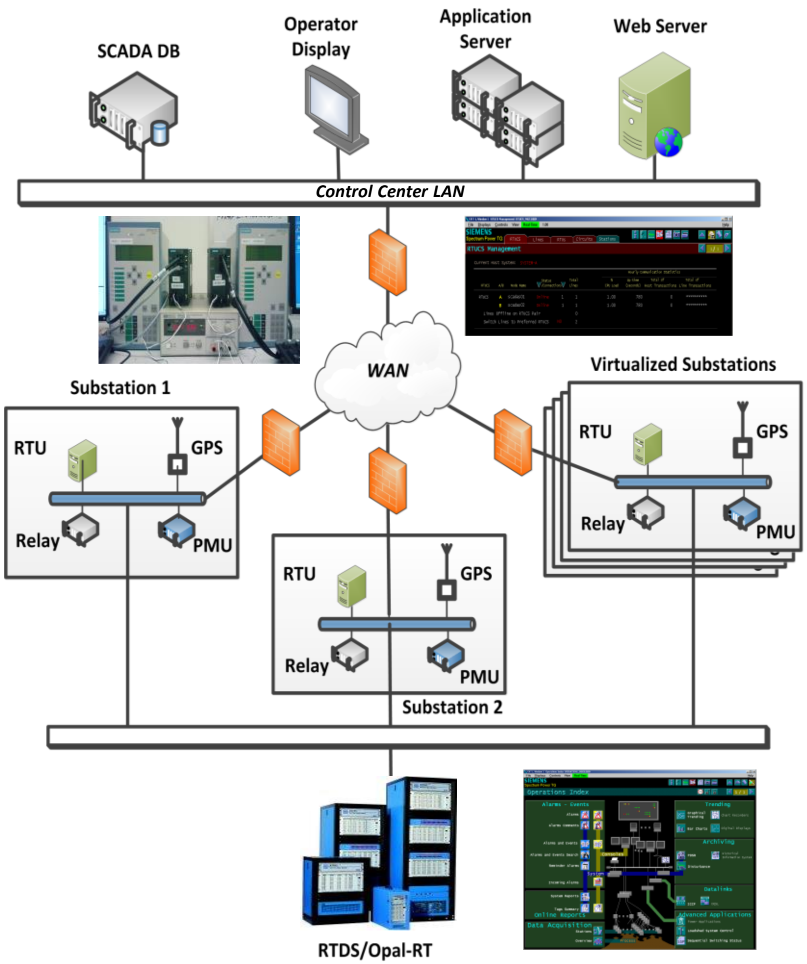
Capabilities

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

Salient Features

1. ***Cyber-in-the-Loop Real-Time Simulatio**n 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.

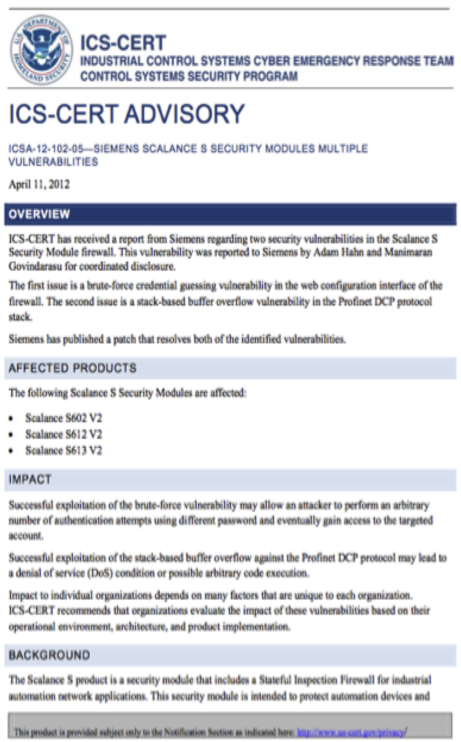
Architecture



ISU *PowerCyber* Testbed - Experiments

CPS Security Testbed – What can we do?

Vulnerability Assessment


ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ADVISORY

ICSA-12-102-05—SIEMENS SCALANCE S SECURITY MODULES MULTIPLE VULNERABILITIES

April 11, 2012

OVERVIEW

ICS-CERT has received a report from Siemens regarding two security vulnerabilities in the Scalance S Security Module firewall. This vulnerability was reported to Siemens by Adam Hahn and Manimaran Govindarasu for coordinated disclosure.

The first issue is a brute-force credential guessing vulnerability in the web configuration interface of the firewall. The second issue is a stack-based buffer overflow vulnerability in the Profinet DCP protocol stack.

Siemens has published a patch that resolves both of the identified vulnerabilities.

AFFECTED PRODUCTS

The following Scalance S Security Modules are affected:

- Scalance S602 V2
- Scalance S612 V2
- Scalance S613 V2

IMPACT

Successful exploitation of the brute-force vulnerability may allow an attacker to perform an arbitrary number of authentication attempts using different password and eventually gain access to the targeted account.

Successful exploitation of the stack-based buffer overflow against the Profinet DCP protocol may lead to a denial of service (DoS) condition or possible arbitrary code execution.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

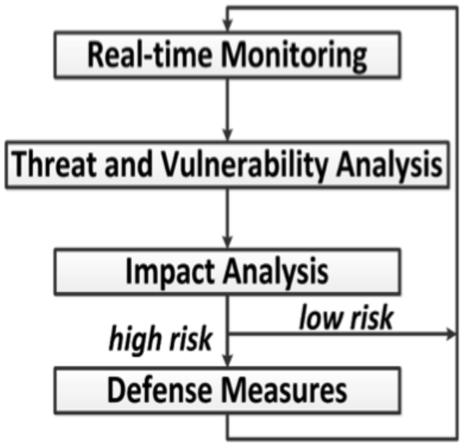
BACKGROUND

The Scalance S product is a security module that includes a Stateful Inspection Firewall for industrial automation network applications. This security module is intended to protect automation devices and

This product is provided subject only to the Notification Section as indicated here: http://www.us-cert.gov/privacy/

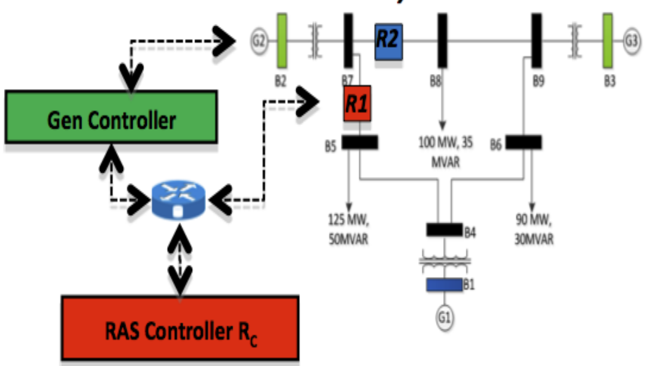
Risk Assessment and Mitigation

- Risk = Threat * Vulnerability * Impacts
- Security Investment Analysis
- Risk Assessment & Risk Mitigation



Attack-Defense Evaluations

Attack on Remedial Action Scheme
WECC 9-bus System



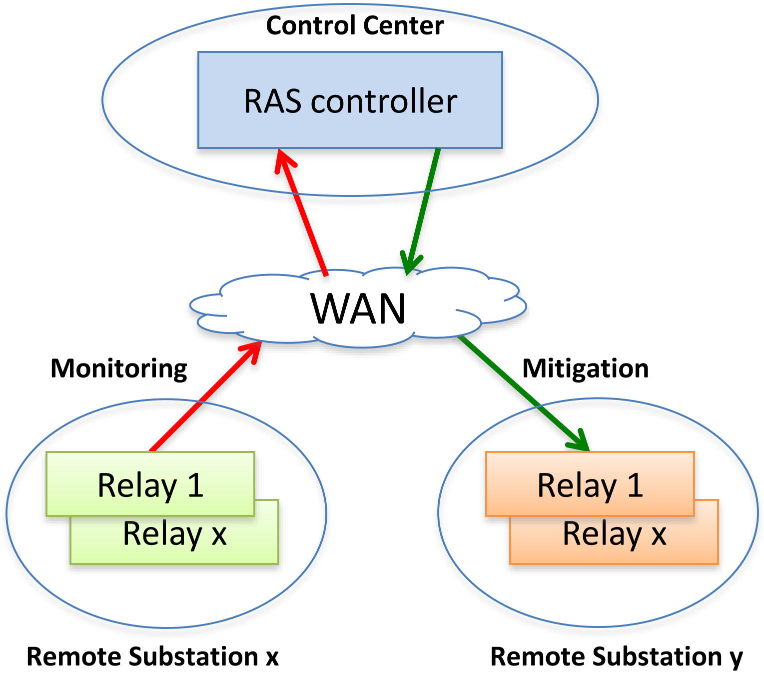
- Data integrity attack to trip R1 + DoS on RAS controller
- R2 trips due to thermal overload; Instability; Load shedding
- Evaluating mitigation schemes

Wide-Area Protection

Remedial Action Schemes (RAS) – Automatic protection systems designed to detect abnormal or predetermined system conditions, and take corrective actions other than and/or in addition to the isolation of faulted components to maintain system reliability.

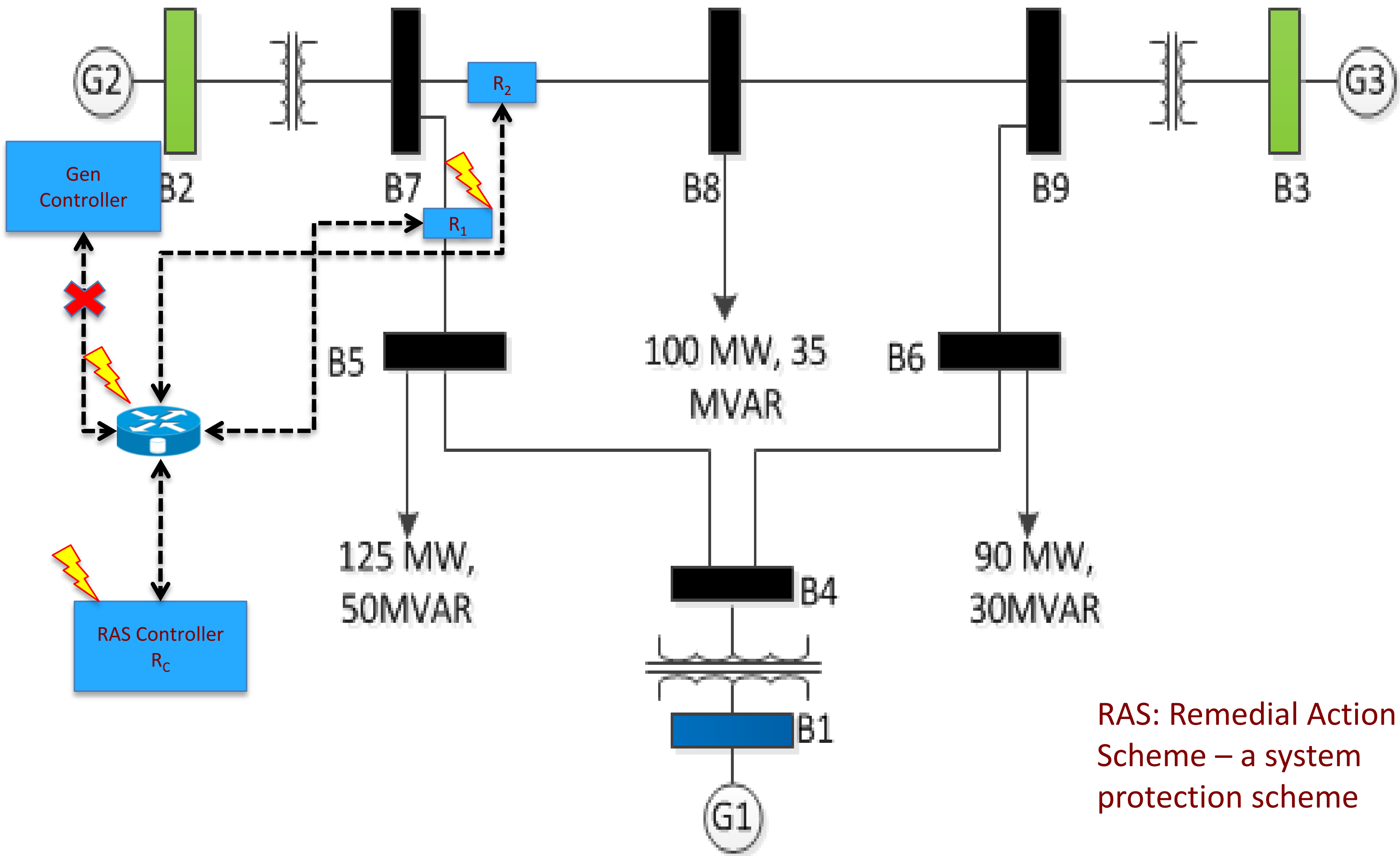
Typical RAS corrective actions are :

- Changes in load (MW)
- Changes in generation (MW and MVAR)
- Changes in system configuration to maintain system stability, acceptable voltage or power flows



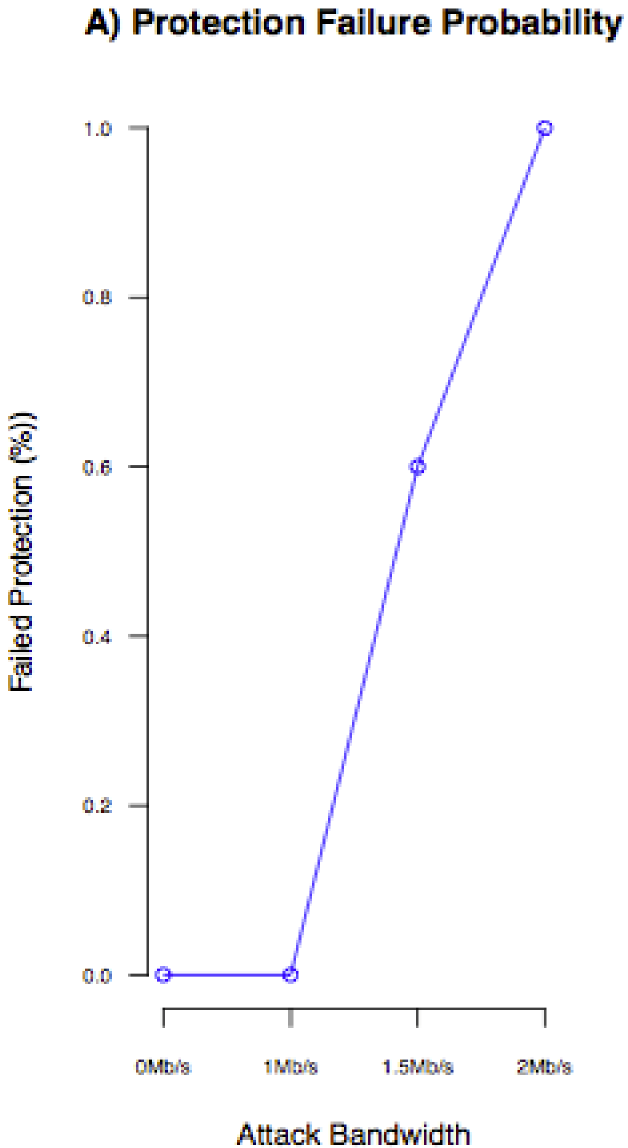
Source: V. Madani, D. Novosel, S. Horowitz, M. Adamiak, J. Amantegui, D. Karlsson, S. Imai, and A. Apostolov, "Ieee psrc report on global industry experiences with system integrity protection schemes (sips)," Power Delivery, IEEE Transactions on, vol. 25, pp. 2143 –2155, oct. 2010.

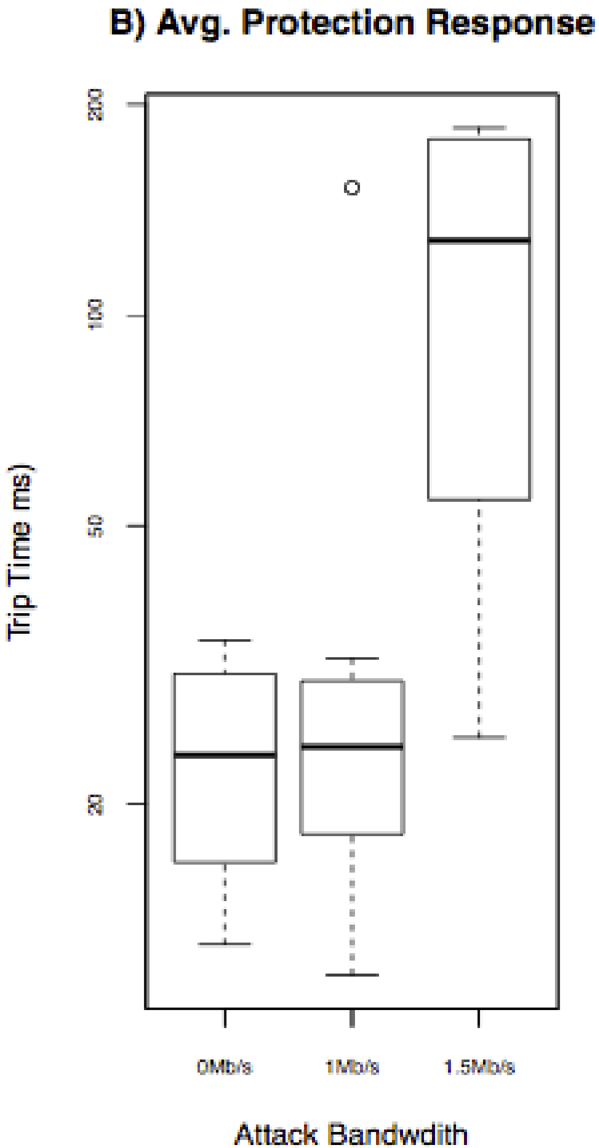
Case Study 1: Coordinated attack on RAS for WECC 9 bus system



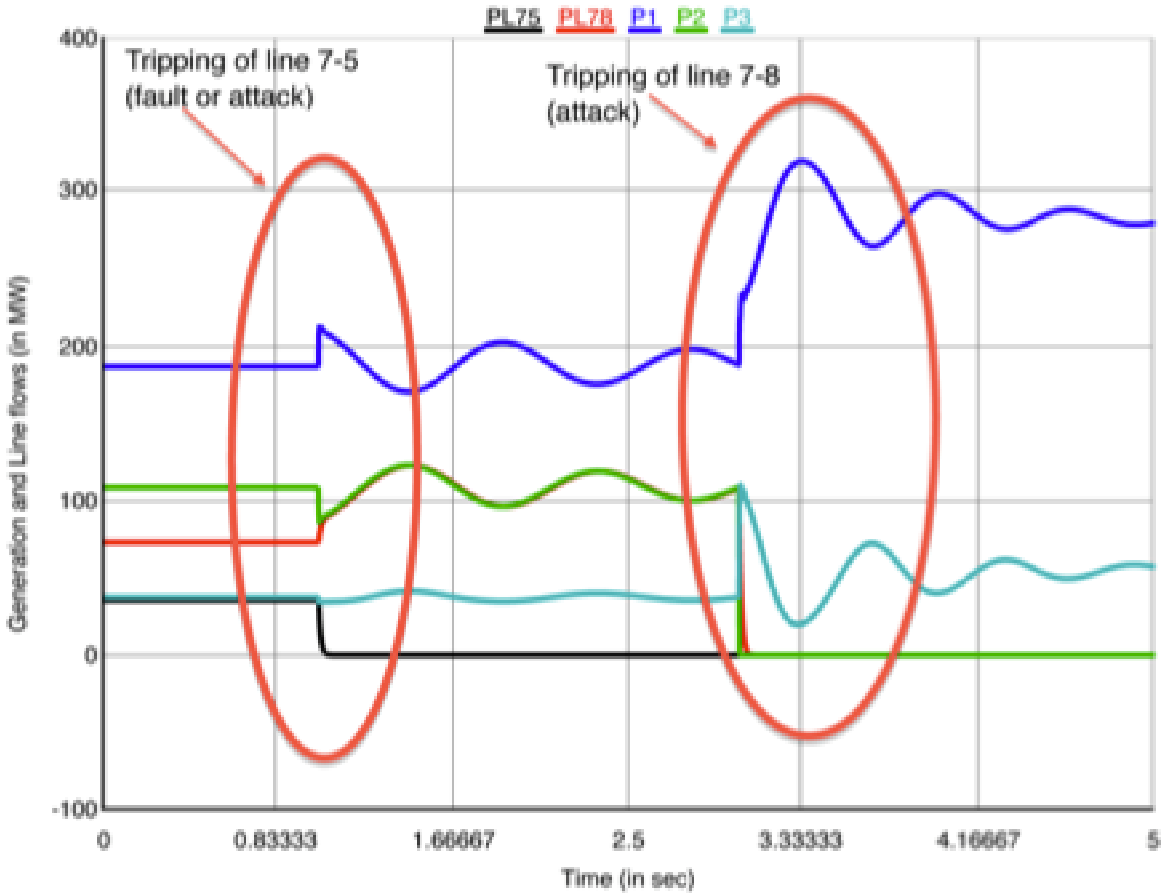
RAS: Remedial Action Scheme – a system protection scheme

DoS on RAS Controller (Relay)





Power system Impacts



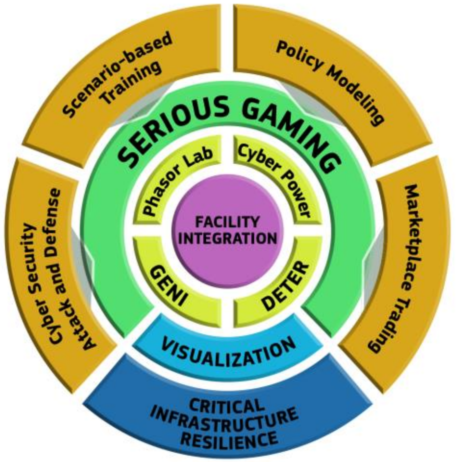
CPS Testbed Federation for Smart Grid: Cyber Security & Resiliency

SmartEnergy CPS

http://smartamerica.org/teams/smart-energy-cps

SmartAmerica Challenge

http://smartamerica.org



This project is funded in part by the NSF and DHS

(NSF Award #s: CNS 1329915, ECCS 1202542, ACI 1346285)

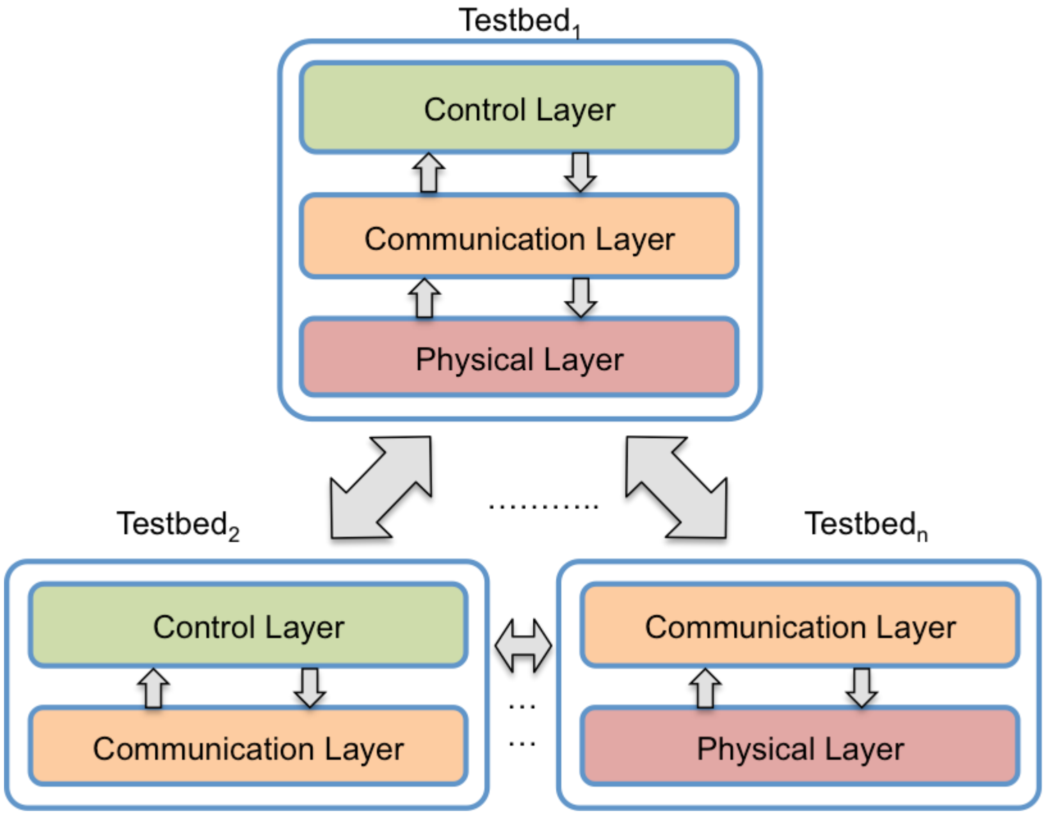
IOWA STATE UNIVERSITY
Department of Electrical and Computer Engineering

USC Viterbi
School of Engineering

MITRE

Testbeds Federation

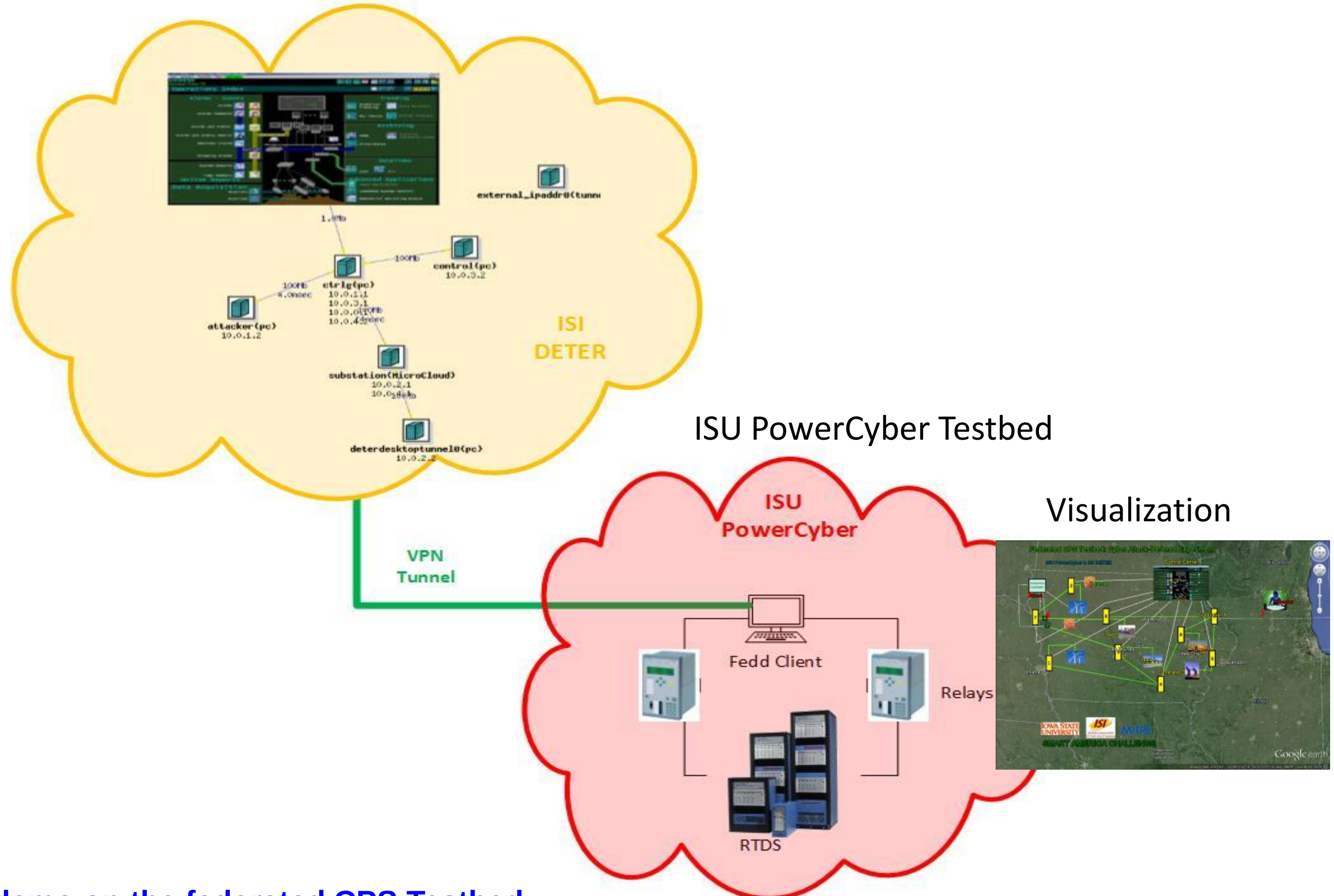
- **Federation** – the concept of combining several individual testbed labs across educational institutions and research labs to leverage resources and achieve synergy with reasonable test systems.



CPS Testbed Federation Architecture

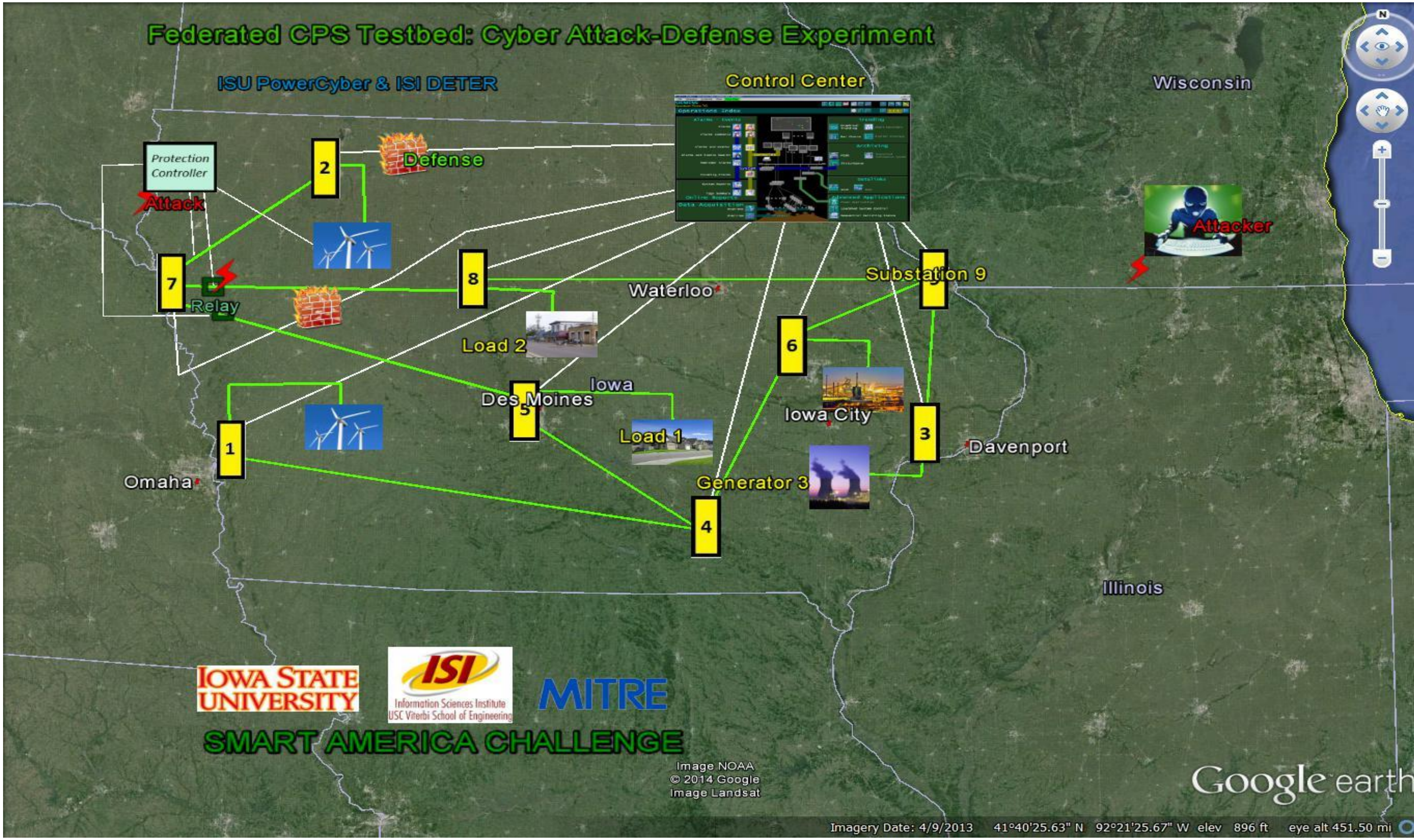
Smart Energy CPS
ISU PowerCyber + ISI DeterLab

USC/ISI DETER Testbed



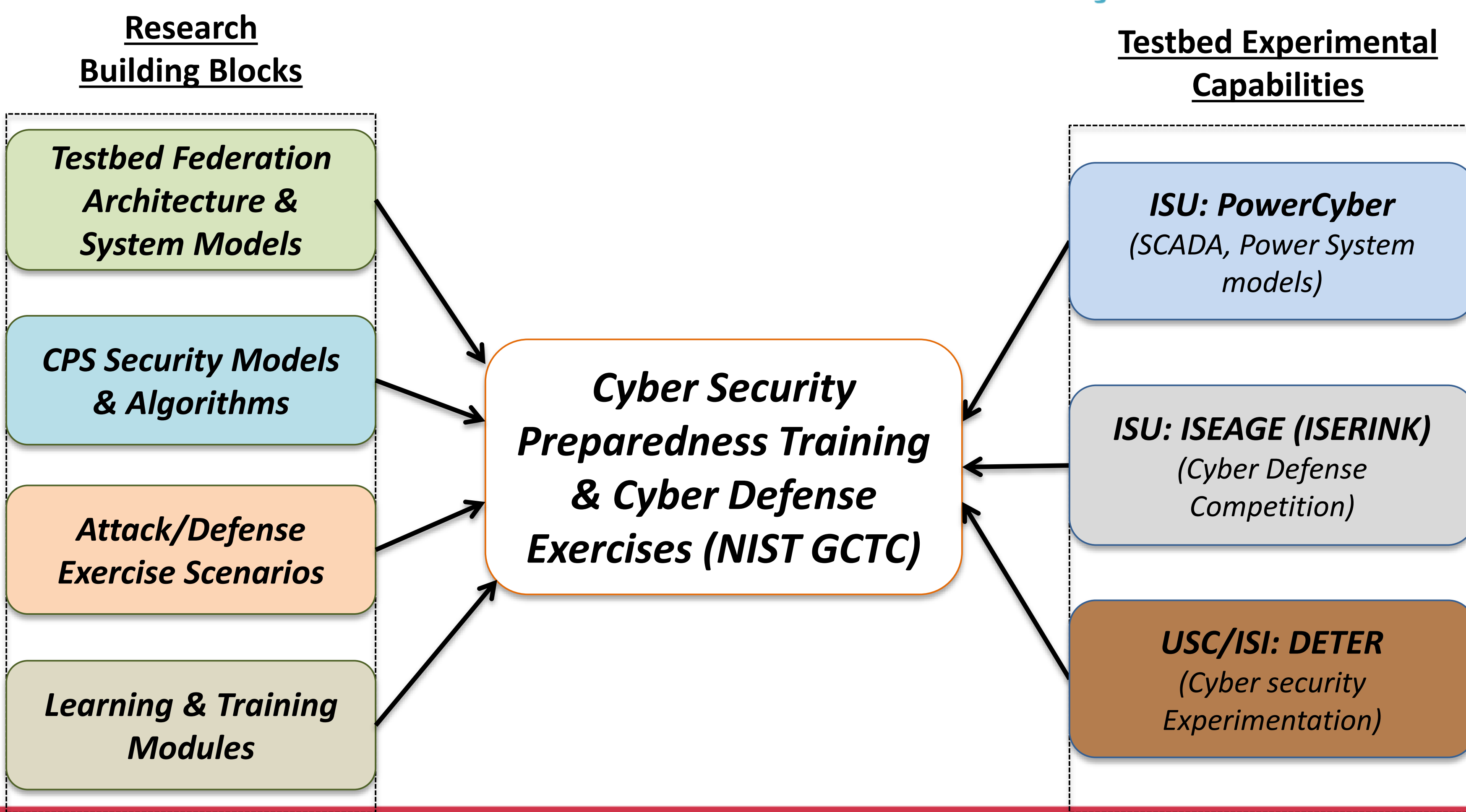
[Attack-defense demo on the federated CPS Testbed]()

Visualization of Attack-Defense on RAS Scheme

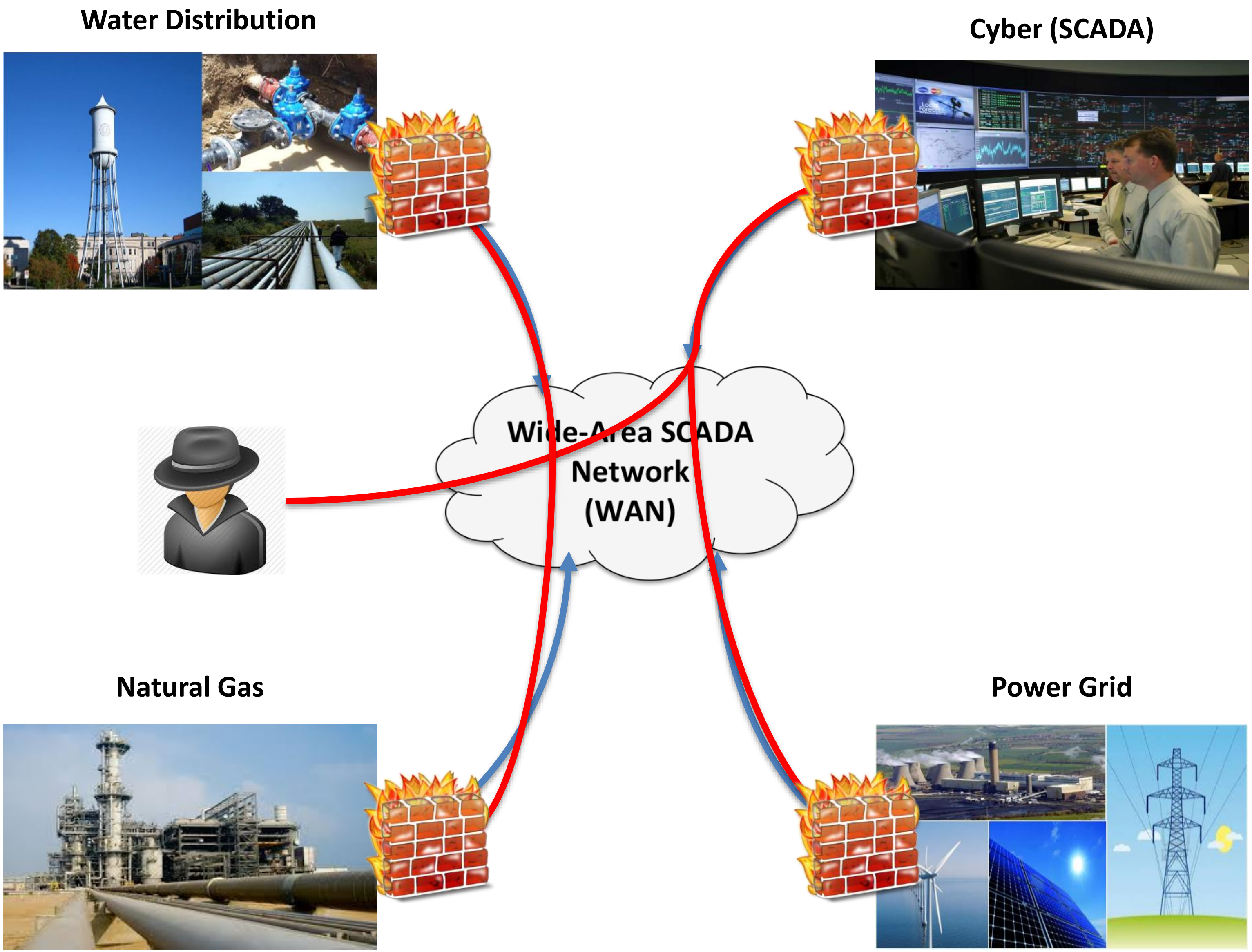


NIST-US Ignite Global City Teams Challenge, 2015

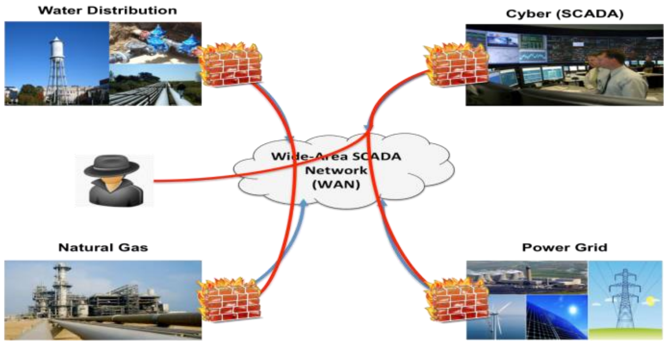
CyDECS: Cyber Defense Exercise (CDE) for Critical Infrastructures Security

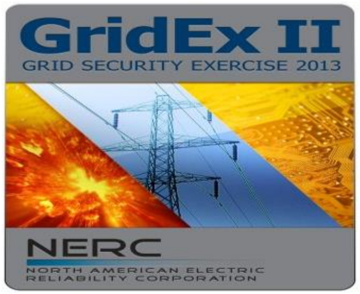


Motivation for CPS-CDE



CDE: Tabletop → Testbed-based

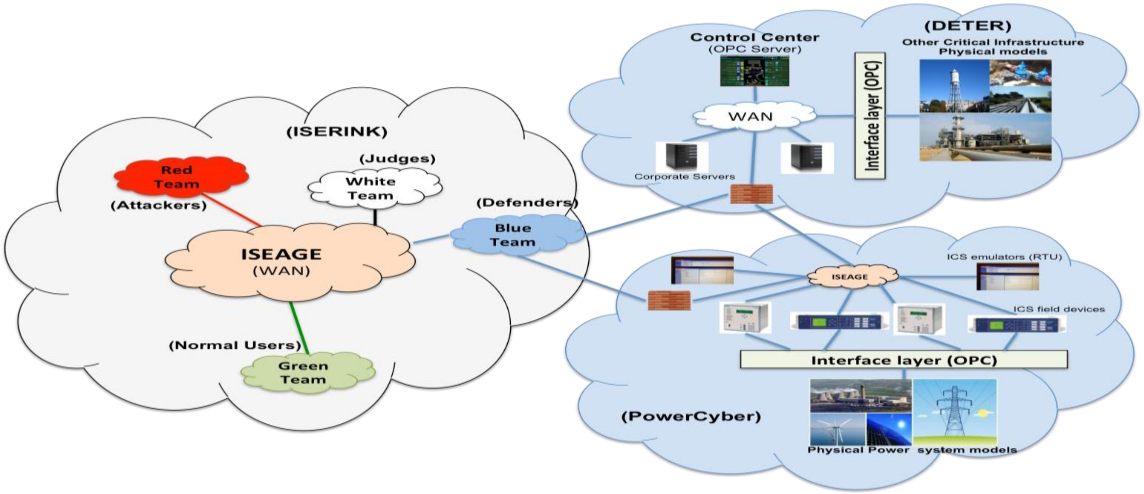




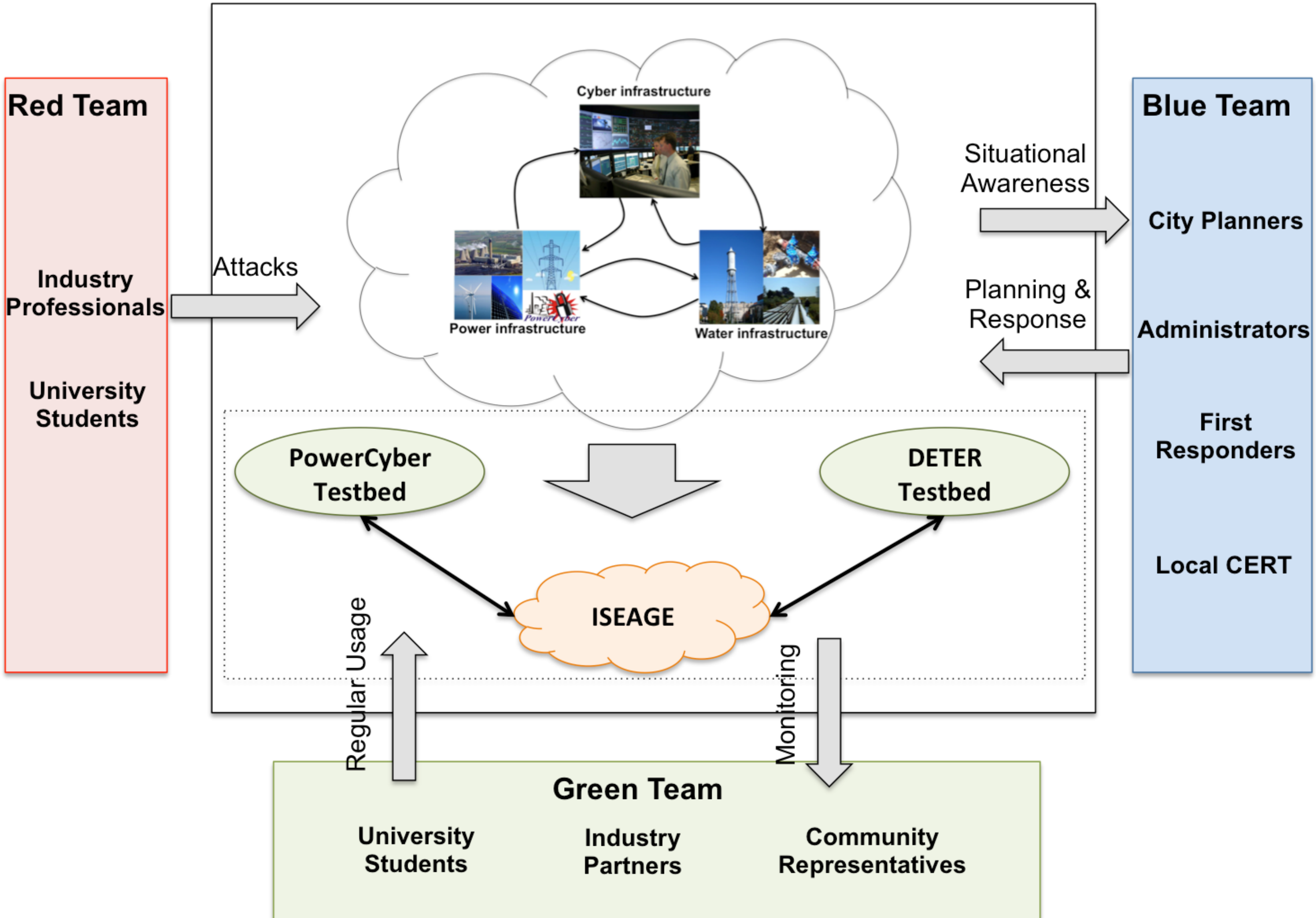
Critical Infrastructure Cyber Security and Cyber Defense

Current solution: Passive, Table-top Cyber Defense Exercise

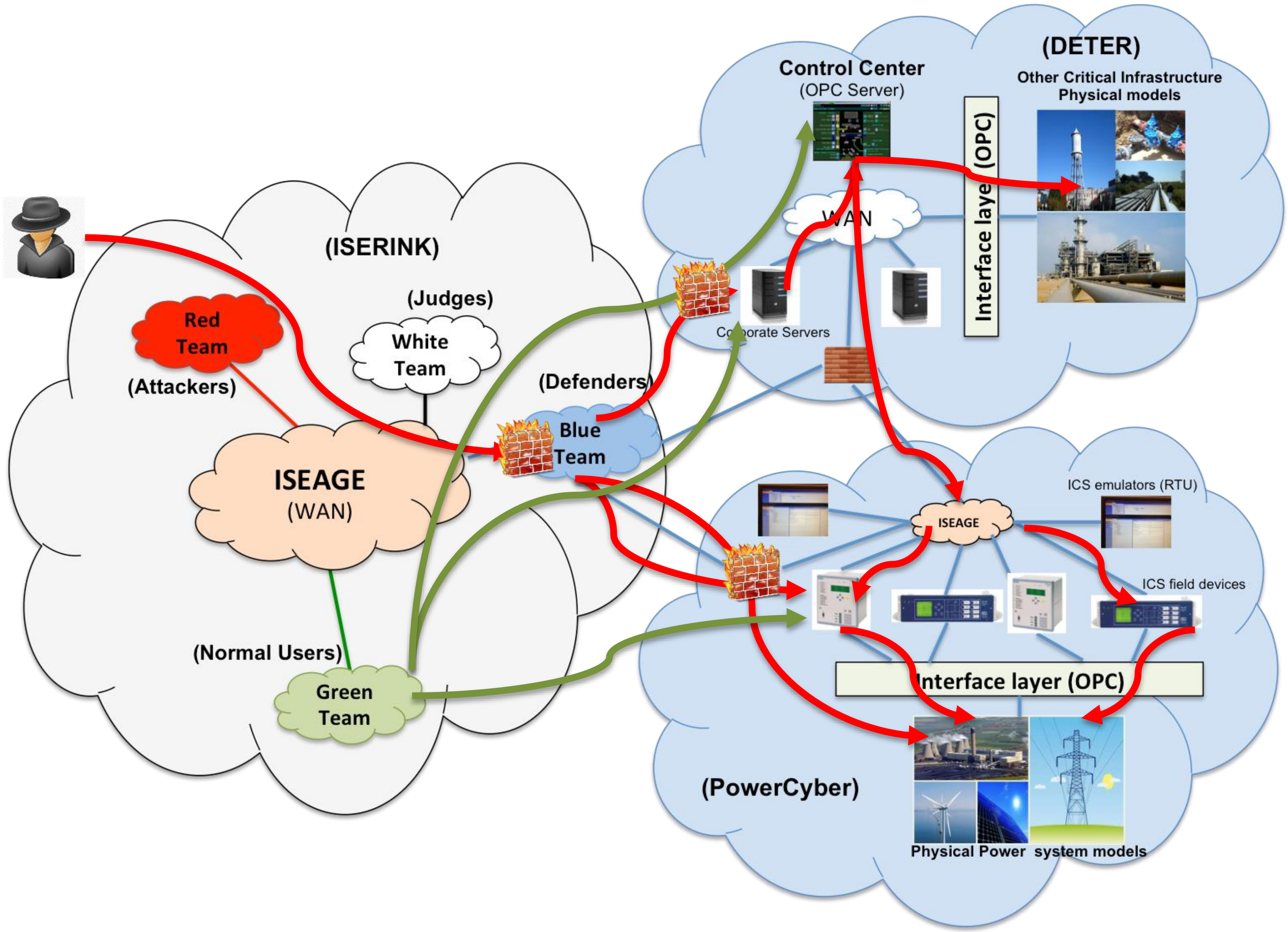
Proposed project: CyDECS - Realistic, Live Cyber Attack/Defense Exercises for multiple Critical Infrastructures on a federated CPS Security Testbed environment



CDE: Concept Diagram



CDE: Use case scenarios



Conclusion

- Science of Experimentation & Testbed Architectures
- CPS testbeds capture interactions between **Cyber-Control-Physi**cal subsystems
- Hybrid model of ***Physical, Emulated, Simulated, and Virtual*** components are needed to build a scalable, high-fidelity, cost-effective CPS testbed
- Testbed based research helps to perform
  - Vulnerability assessment for devices, systems and protocols
  - Impact analysis of cyber events on physical systems
  - Attack-Defense Evaluation and validation
- Testbeds can be leveraged to conduct **R&D, education, industry training and cyber defense competitions**

Future Research Opportunities

- Large-scale, high-fidelity CPS Security Testbed
  - Testebed Federations, models, libraries, datasets
  - Regional, National-scale experiments
  - International Collaboration
- NERC GridEx-type Attack-Defense Evaluations
  - Advanced Persistent Threats
  - Robust Countermeasures
  - Collaboration with industry and NERC
- Critical Infrastructure Resiliency preparedness
  - Table-top exercises for critical infrastructures security
- CPS Cyber Defense Competition

Future Research Opportunities

1

- **Large-scale high-fidelity, federated CPS testbed**
- Remote and open access
- Experiment design
- Accelerate R&D, education, and workforce development

2

- **CPS Cloud architecture, algorithms, and services**
- Scalable architecture and sustainable model
- Promotes collaboration thro resource sharing

3

- **Testebed for interdependent CPS sectors**
- Power grid, oil and natural gas, transportation, water distribution
- Remote and open access

THANK YOU …

Acknowledgements

Sponsors:

- National Science Foundation (NSF) - CPS, ECCS, SaTC Programs
- Department of Homeland Security (DHS)
- Department of Energy (DOE)
- NSF IU/CRC Power Engineering Research Center (PSERC)
- Iowa State University (ISU) Electric Power Research Center (EPRC)

Collaborators:

Prof. Chen-Ching Liu, Washington State University (WSU)
Prof. Venkat Ajjarapu & Prof. Doug Jacobson, ISU
Adam Hahn, WSU & S. Sridhar, PNNL & Junho Hong, ABB
Terry Benzel, Alefiya Hussain, Ryan Goodfellow, USC/ISI

Students:

Aditya Ashok (ISU), Siddharth Sridhar (ISU/PNNL), Matt Brown (ISU)
Aswin Chidambaram (ISU), Pengyuan Wang (ISU),
Sujatha Krishnaswamy (ISU), Alexandru Ştefanov (UC Dublin)

Professional:

IEEE PES - PSACE CAMS Cyber Security Task Force