GIAN Short course

Cyber-Physical Security for the Smart Grid

Indian Institute of Technology, Bombay, India

Coordinator: Prof. R. K. Shyamasundar

Manimaran Govindarasu

Dept. of Electrical and Computer Engineering

Iowa State University

Email: gmani@iastate.edu

http://powercyber.ece.iastate.edu

March 5-16, 2018

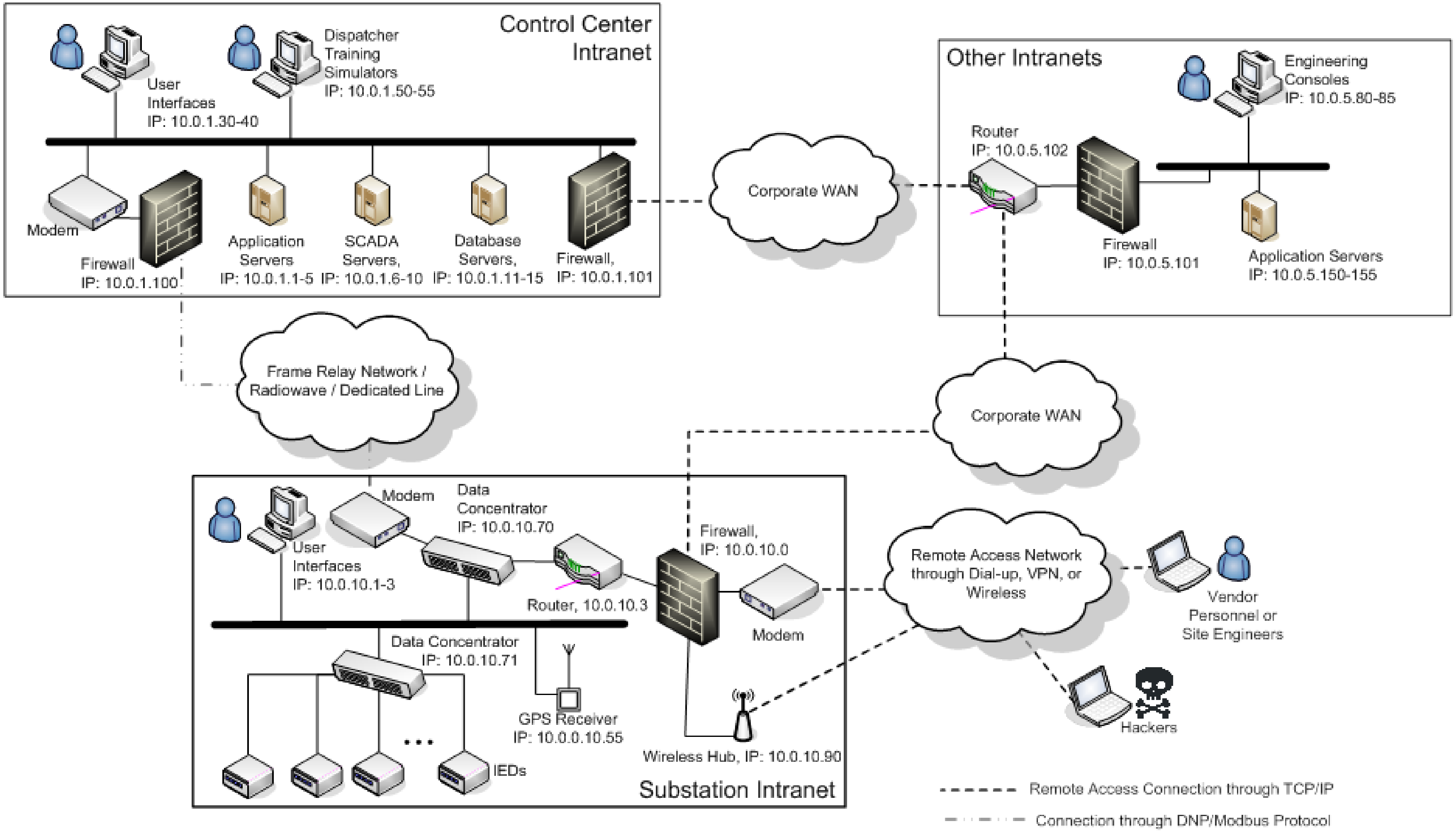
Course Agenda

Day 01	• Module 1: Cyber Threats, Attacks, and Security concepts
Day 02	• Module 2: Risk Assessment and Mitigation & • Overview of Indian Power Grid
Day 03	• Module 3: Attack-resilient Wide-Monitoring, Protection, Control
Day 04	• Module 4: SCADA, Synchrophasor, and AMI Networks & Security
Day 05	• Module 5: Attack Surface Analysis and Reduction Techniques
Day 06	• Module 6: CPS Security Testbeds & Case Studies
Day 07	• Module 7: Cybersecurity Standards & Industry Best Practices
Day 08	• Module 8: Cybersecurity Tools & Vulnerability Disclosure
Day 09	• Module 9 : Review of materials, revisit case studies, assessments
Day 10	• Module 10: Research directions, education and training

Outline of **Module 6**

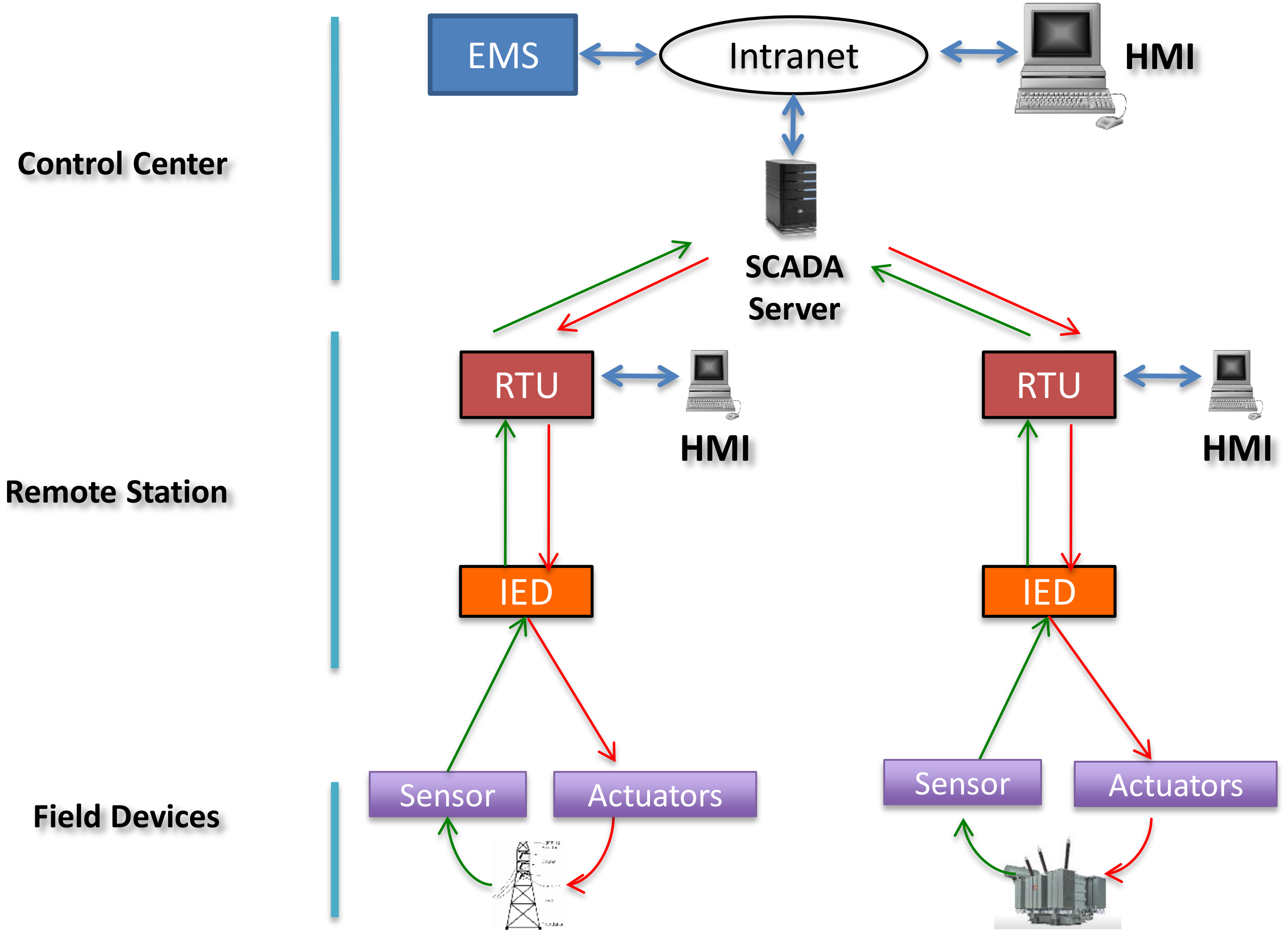
- Testbed Concepts & Architecture
- Case Study – Iowa State's *PoweCyber Security*
- *Case Study* – IIT Bombay's *WAMS Testbed (Demo)*
- Testbed R&D needs
- Testbed Demos

SCADA Control Network – A schematic



Control Center Intranet
User Interfaces IP: 10.0.1.30-40
Dispatcher Training Simulators IP: 10.0.1.50-55
Modem
Firewall IP: 10.0.1.100
Application Servers IP: 10.0.1.1-5
SCADA Servers, IP: 10.0.1.6-10
Database Servers, IP: 10.0.1.11-15
Firewall, IP: 10.0.1.101
Corporate WAN
Other Intranets
Router IP: 10.0.5.102
Engineering Consoles IP: 10.0.5.80-85
Firewall IP: 10.0.5.101
Application Servers IP: 10.0.5.150-155
Frame Relay Network / Radiowave / Dedicated Line
Corporate WAN
Modem
Data Concentrator IP: 10.0.10.70
User Interfaces IP: 10.0.10.1-3
Firewall, IP: 10.0.10.0
Router, 10.0.10.3
Modem
Remote Access Network through Dial-up, VPN, or Wireless
Vendor Personnel or Site Engineers
Data Concentrator IP: 10.0.10.71
GPS Receiver IP: 10.0.0.10.55
Wireless Hub, IP: 10.0.10.90
Hackers
IEDs
Substation Intranet
Remote Access Connection through TCP/IP
Connection through DNP/Modbus Protocol

SCADA Operation



Control Center

EMS

Intranet

HMI

SCADA Server

Remote Station

RTU

HMI

IED

RTU

HMI

IED

Field Devices

Sensor

Actuators

Sensor

Actuators

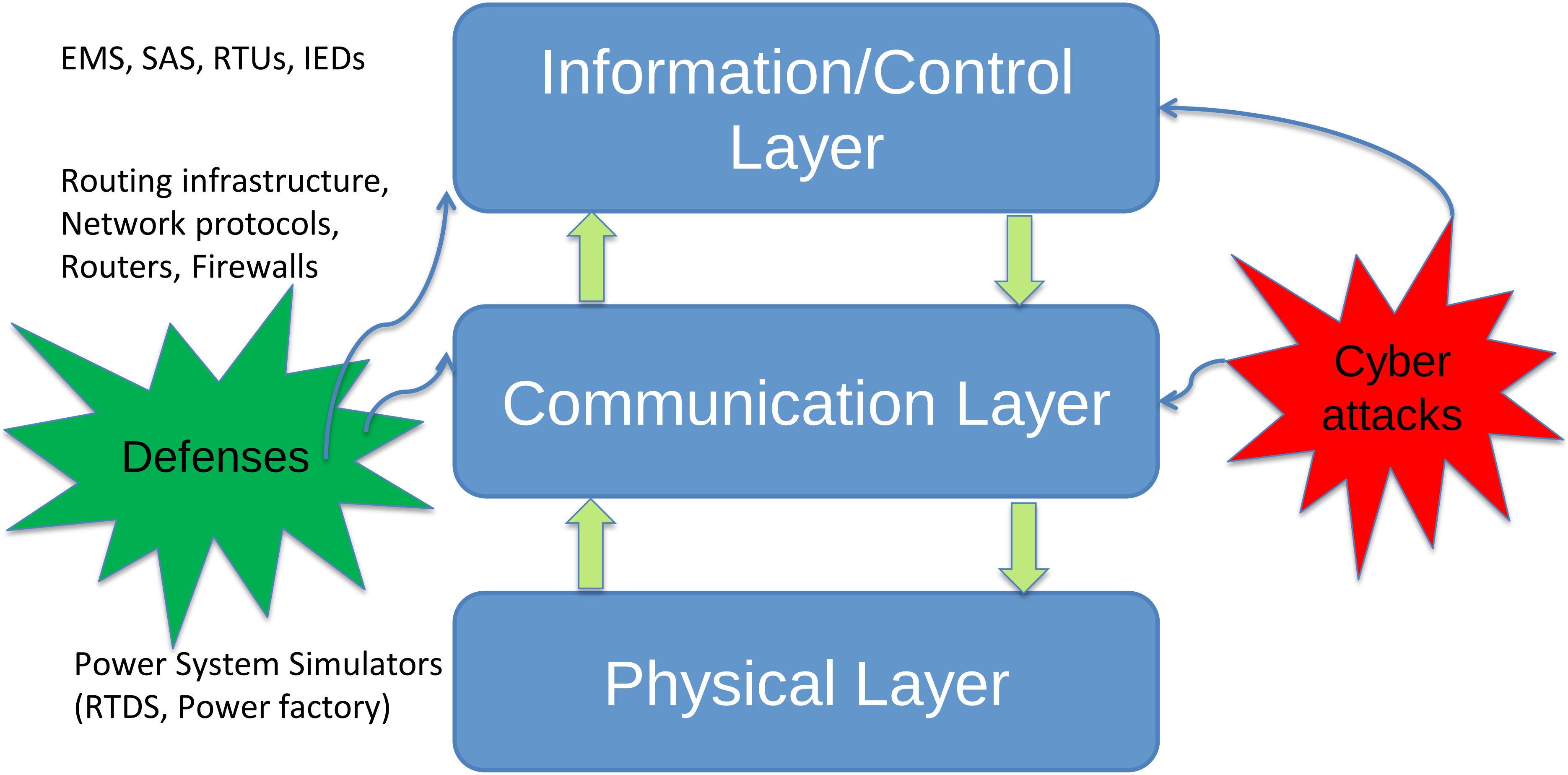
Testbed Definition

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

Motivation for Testbeds

- Realistic platform for model validation
  - Power system dynamics
  - Communication system dynamics
  - Control applications
- Realistic platform for experimental evaluation
  - Cyber-Control-Physical interactions
  - Evaluation of CPS architectures, models, and algorithms
  - Design, build, test, evaluate and deploy
- Accelerate Innovation
  - Realism, Fidelity, Programmability, Repeatability, Resource sharing
- Bridge Theory and Practice
- Pathway from Academic Research to Industry Practice

CPS Security Testbed – A Conceptual View

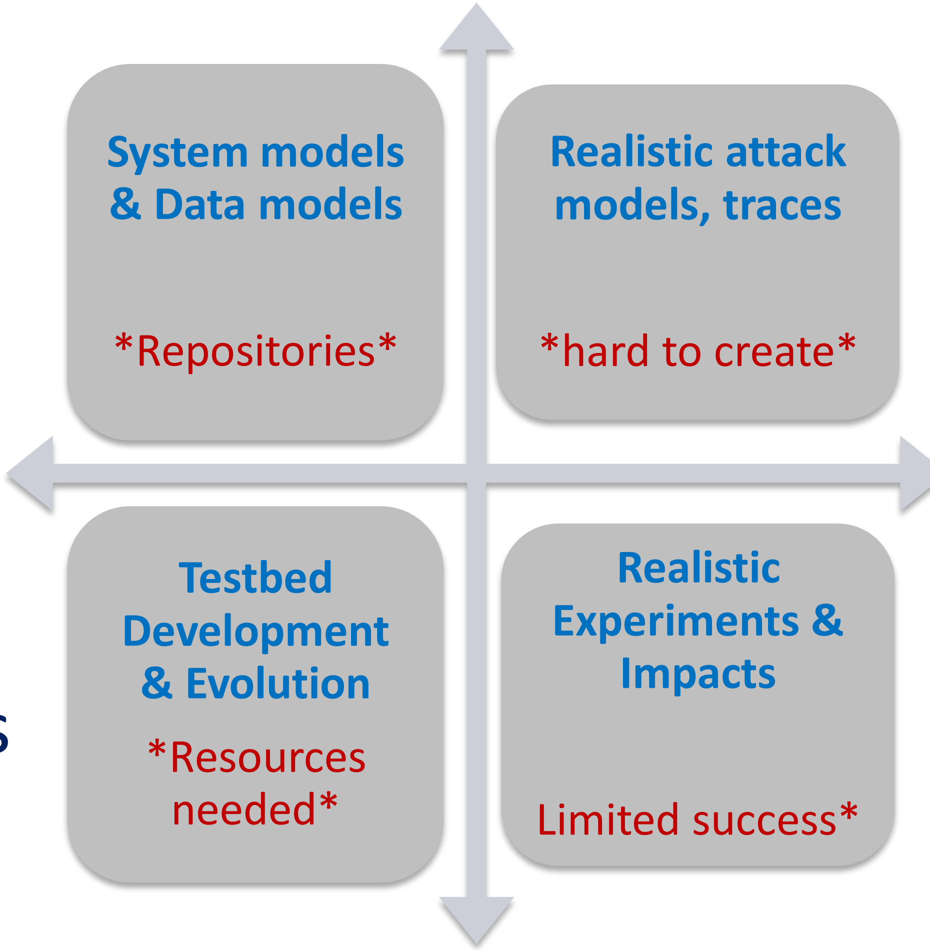

EMS, SAS, RTUs, IEDs
Information/Control Layer
Routing infrastructure, Network protocols, Routers, Firewalls
Communication Layer
Defenses
Cyber attacks
Power System Simulators (RTDS, Power factory)
Physical Layer

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
- Re-configurability
- Interoperability
- Federation
- Standard models, datasets
- Open, Remote access?



System models & Data models

Repositories

Realistic attack models, traces

hard to create

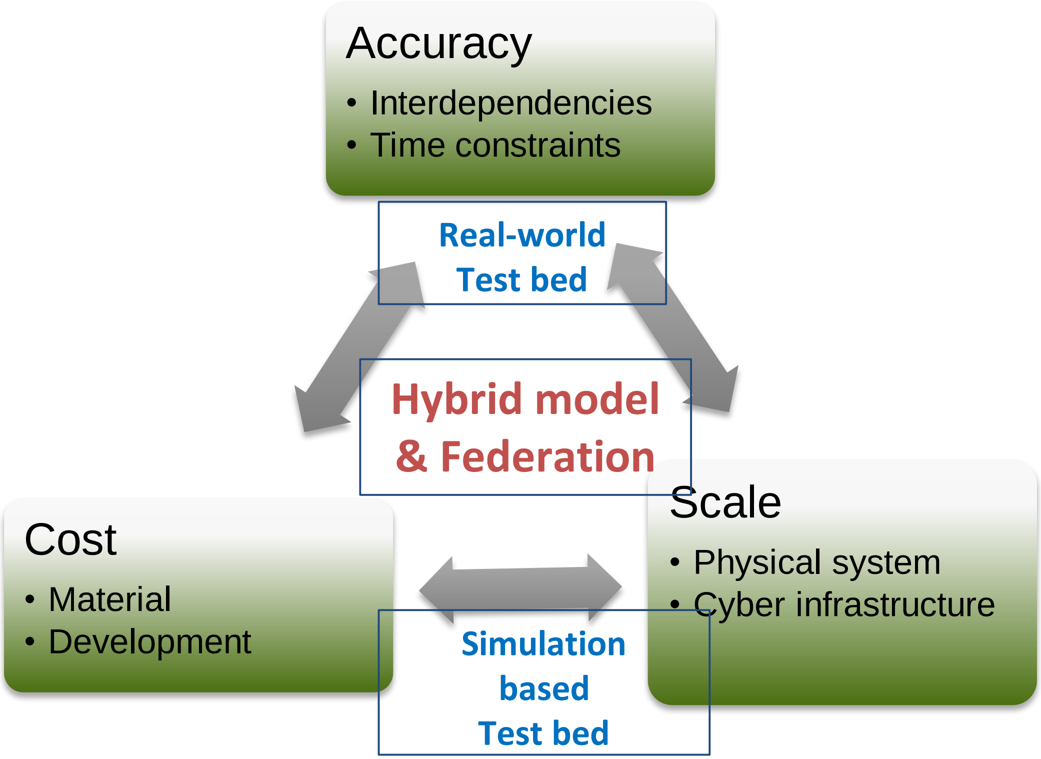
Testbed Development & Evolution

Resources needed

Realistic Experiments & Impacts

Limited success*

Testbeds & Design Tradeoffs



Accuracy
- Interdependencies
- Time constraints

Real-world Test bed

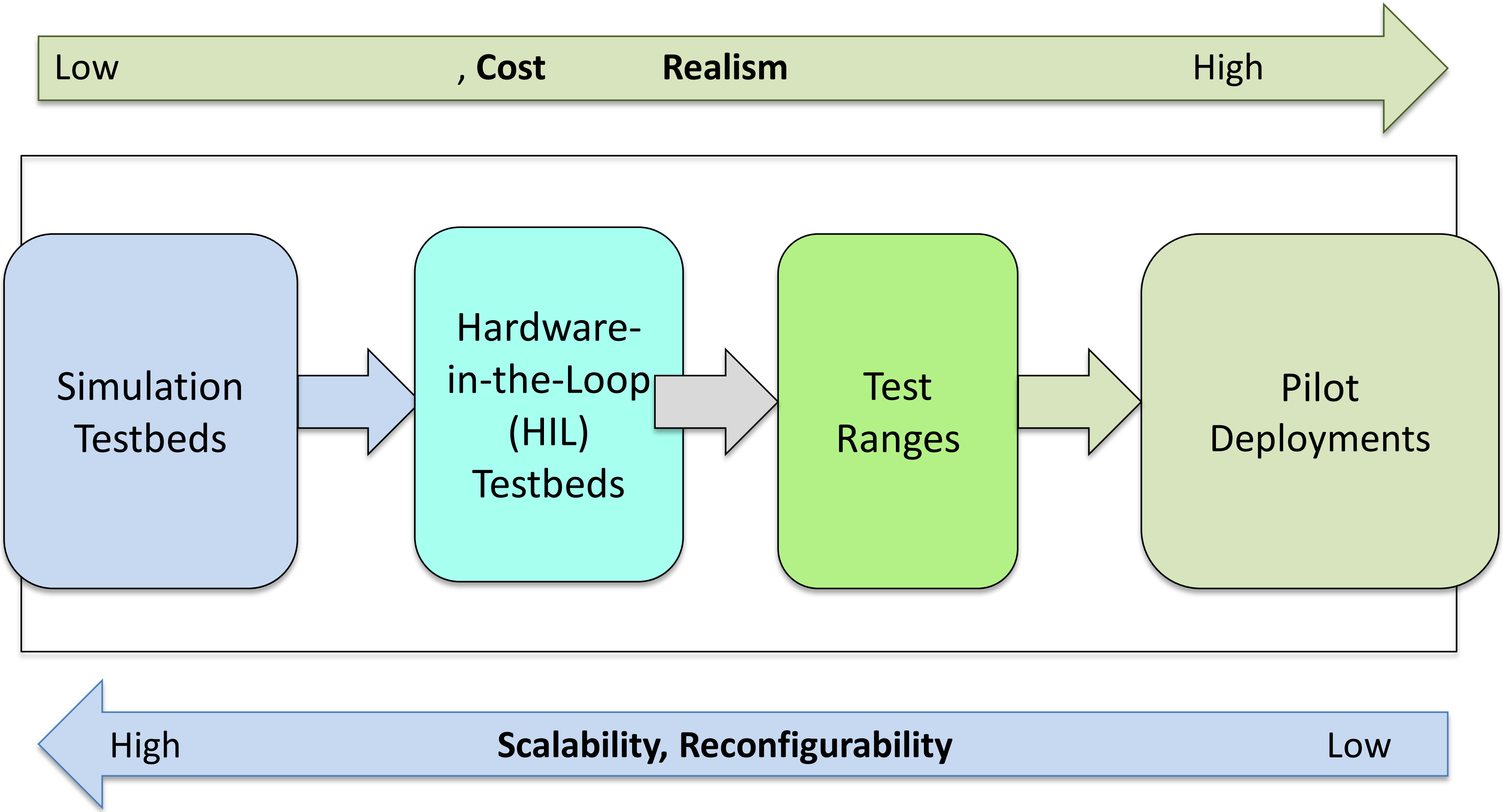
Hybrid model & Federation

Cost
- Material
- Development

Scale
- Physical system
- Cyber infrastructure

Simulation based Test bed

…. Testbed spectrum ….



Low , Cost Realism High

Simulation Testbeds

Hardware-in-the-Loop (HIL) Testbeds

Test Ranges

Pilot Deployments

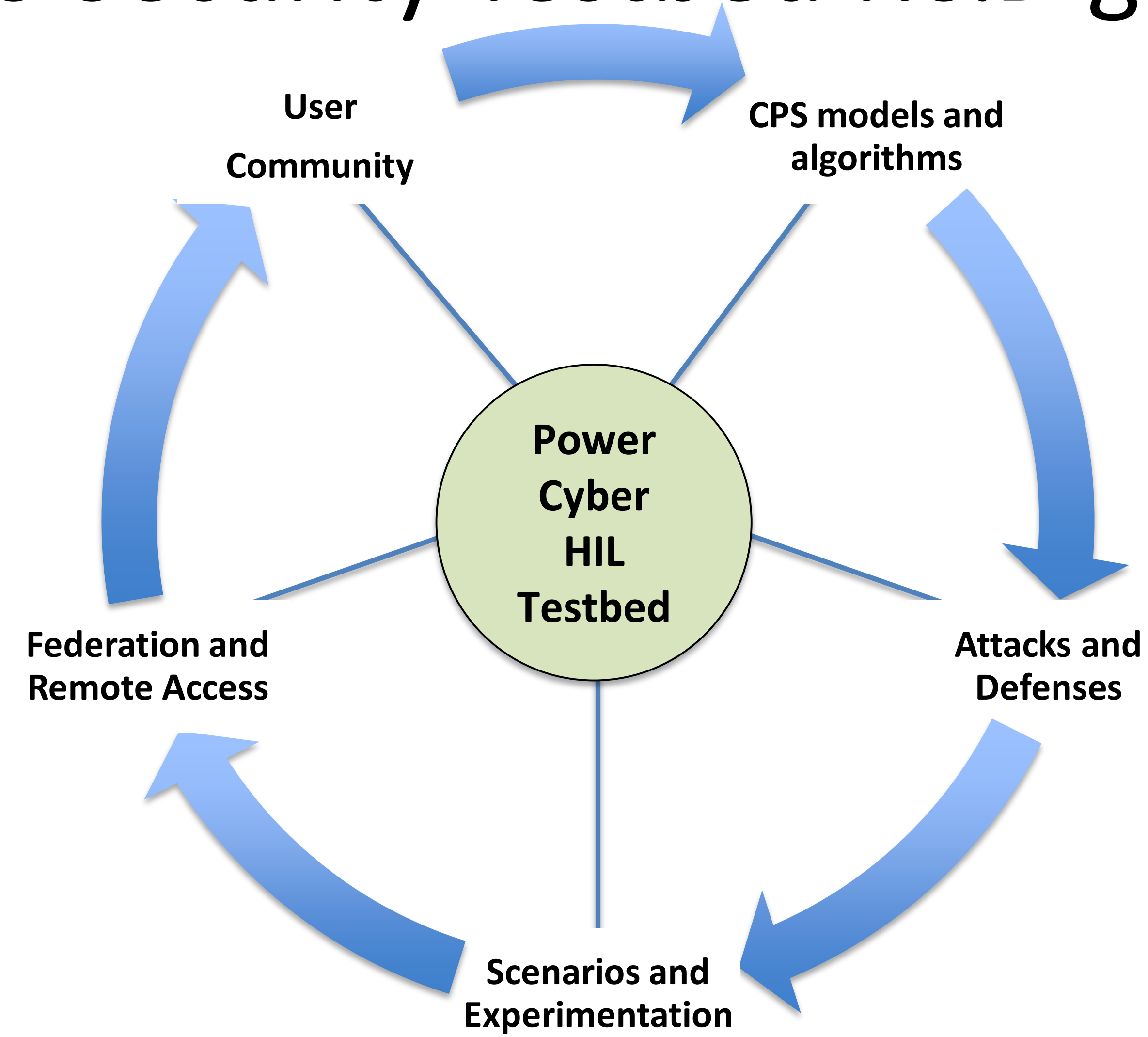
High Scalability, Reconfigurability Low

Some key objectives for Testbed R&D

- Develop innovative testbed architectures and abstractions for large-scale realistic CPS security testbeds

- Design, implementation, and deployment of a high-fidelity, scalable, open-access testbed for research experimentation

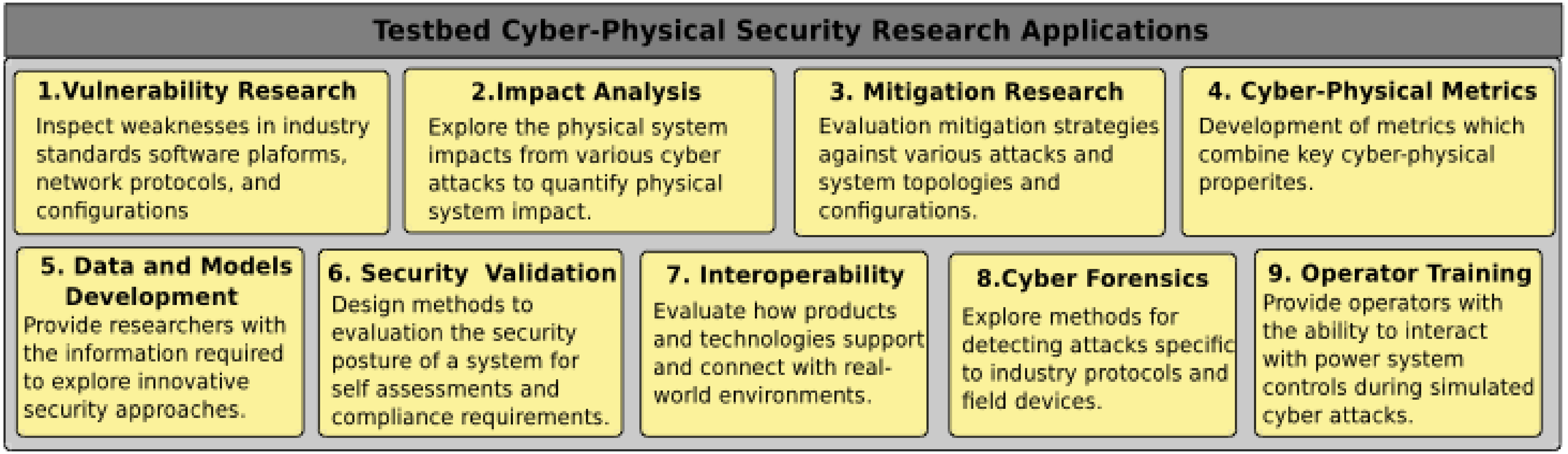
CPS Security Testbed R&D goals


User
Community
CPS models and algorithms
Power Cyber HIL Testbed
Attacks and Defenses
Scenarios and Experimentation
Federation and 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

Testbed – a validation platform



Testbed Cyber-Physical Security Research Applications

1.Vulnerability Research
Inspect weaknesses in industry standards software plaforms, network protocols, and configurations

2.Impact Analysis
Explore the physical system impacts from various cyber attacks to quantify physical system impact.

3. Mitigation Research
Evaluation mitigation strategies against various attacks and system topologies and configurations.

4. Cyber-Physical Metrics
Development of metrics which combine key cyber-physical properites.

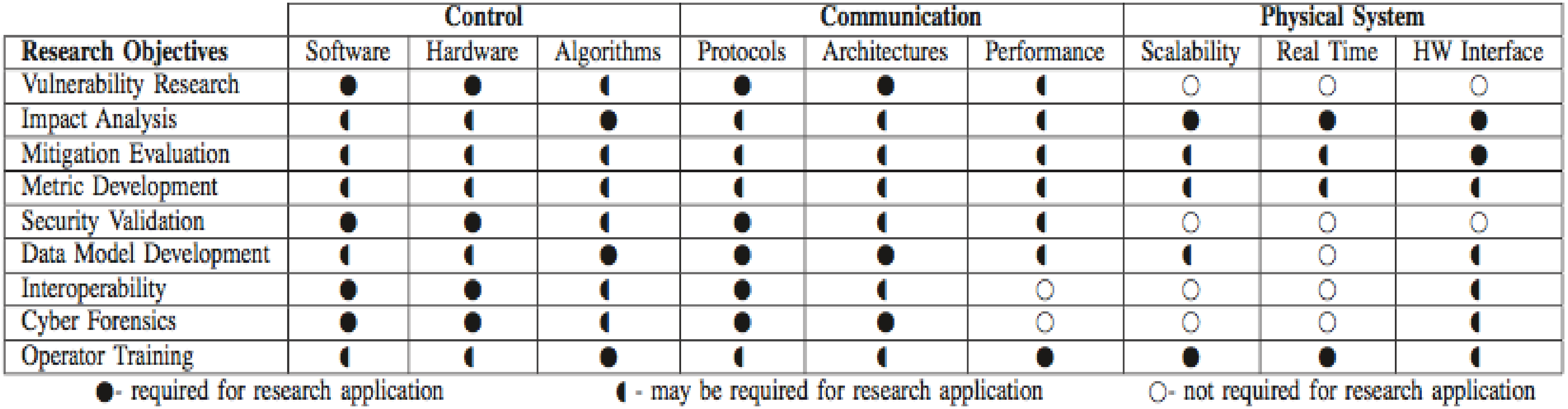
5. Data and Models Development
Provide researchers with the information required to explore innovative security approaches.

6. Security Validation
Design methods to evaluation the security posture of a system for self assessments and compliance requirements.

7. Interoperability
Evaluate how products and technologies support and connect with real-world environments.

8.Cyber Forensics
Explore methods for detecting attacks specific to industry protocols and field devices.

9. Operator Training
Provide operators with the ability to interact with power system controls during simulated cyber attacks.



	Control			Communication			Physical System		
Research Objectives	Software	Hardware	Algorithms	Protocols	Architectures	Performance	Scalability	Real Time	HW Interface
Vulnerability Research	●	●	◖	●	●	◖	○	○	○
Impact Analysis	◖	◖	●	◖	◖	◖	●	●	●
Mitigation Evaluation	◖	◖	◖	◖	◖	◖	◖	◖	●
Metric Development	◖	◖	◖	◖	◖	◖	◖	◖	◖
Security Validation	●	●	◖	●	◖	◖	○	○	○
Data Model Development	◖	◖	●	●	●	◖	◖	○	◖
Interoperability	●	●	◖	●	◖	○	○	○	◖
Cyber Forensics	●	●	◖	●	●	○	○	○	◖
Operator Training	◖	◖	●	◖	◖	●	●	●	◖

●- required for research application ◖ - may be required for research application ○- not required for research application

Adam Hahn, Aditya Ashok, Siddharth Sridhar, Manimaran Govindarasu, *Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid,* IEEE Transactions on Smart Grid. June 2013.

Testbed R&D Tasks

1. CPS Testbed Federation Architecture – Scalability, High-Fidelity, Remote Access
2. Testbed Use-case Experimental Scenarios for CPS Security Experimentation
3. Coordinated Attack/Defense Experimental Validation of Attack-resilient WAMPAC algorithms
4. Vulnerability Assessment and testing of SCADA devices, platforms and network protocols
5. Education: educational modules & industry training modules
6. Outreach: Cyber-Physical System Cyber Defense Competitions (CPS-CDC)
7. Online repository of cyber and power system models, datasets and attack traces

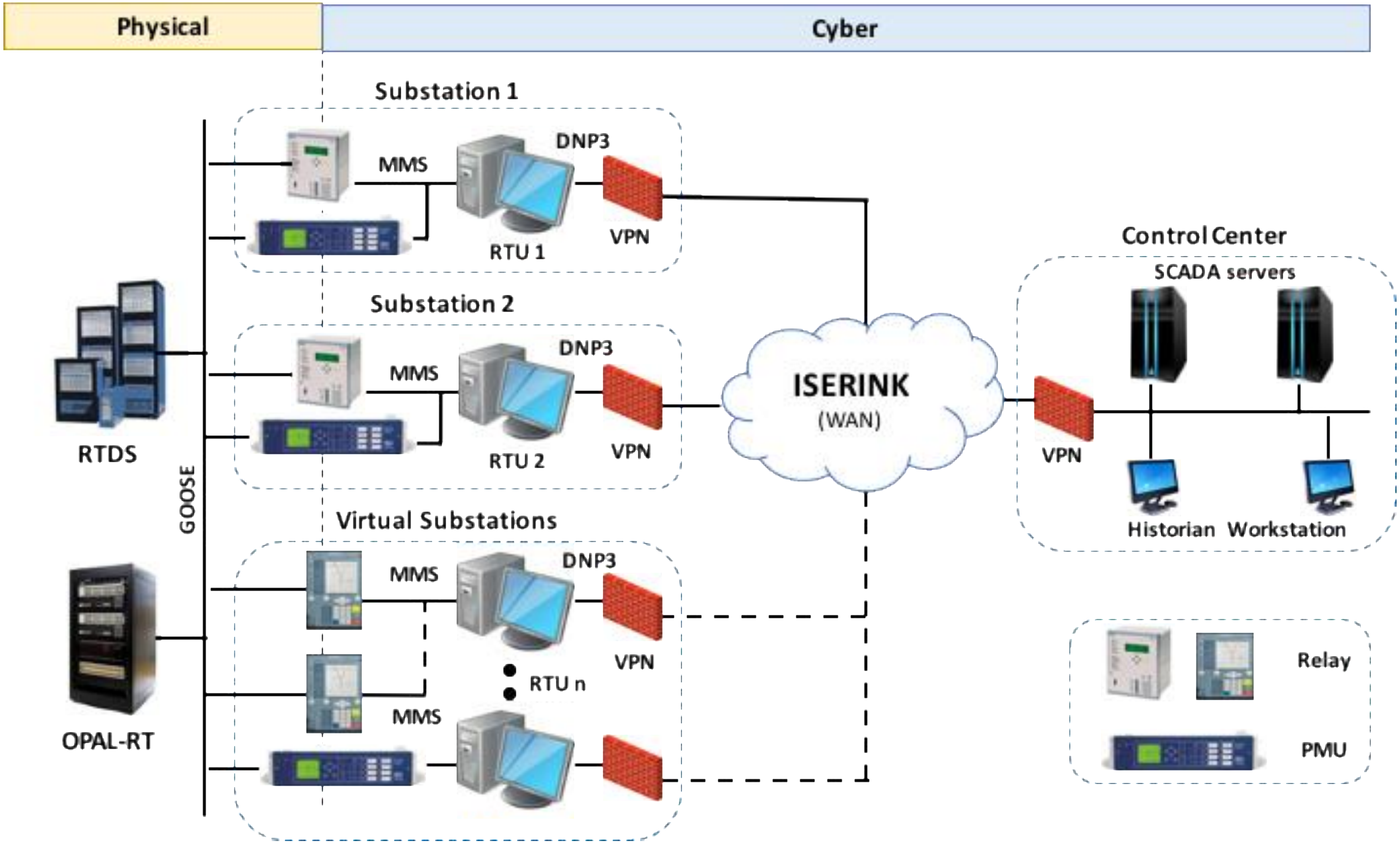
CPS (Security) Testbeds for Smart Grid – Examples

- 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
- WAMS & WAC Testbed @ Indian Institute of Technology (IIT), Bombay

Outline of **Module 6**

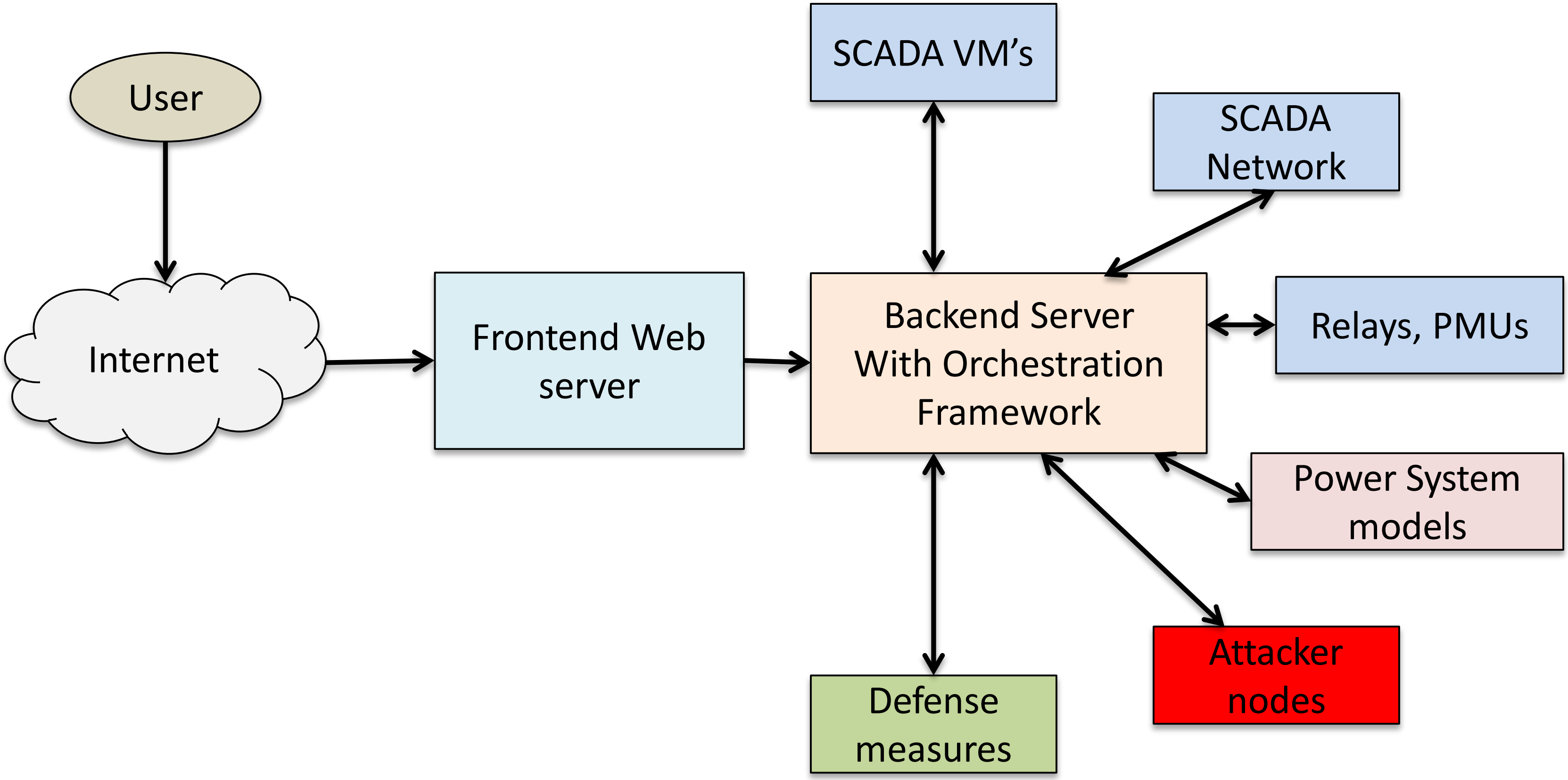
- Testbed Concepts & Architecture
- Case Study & Demo – Iowa State's *PoweCyber Security*
- *Case Study* – IIT Bombay's *WAMS Testbed (Demo)*
- Testbed R&D needs
- Testbed Demos

Iowa State's *PowerCyber:* A CPS Security Testbed

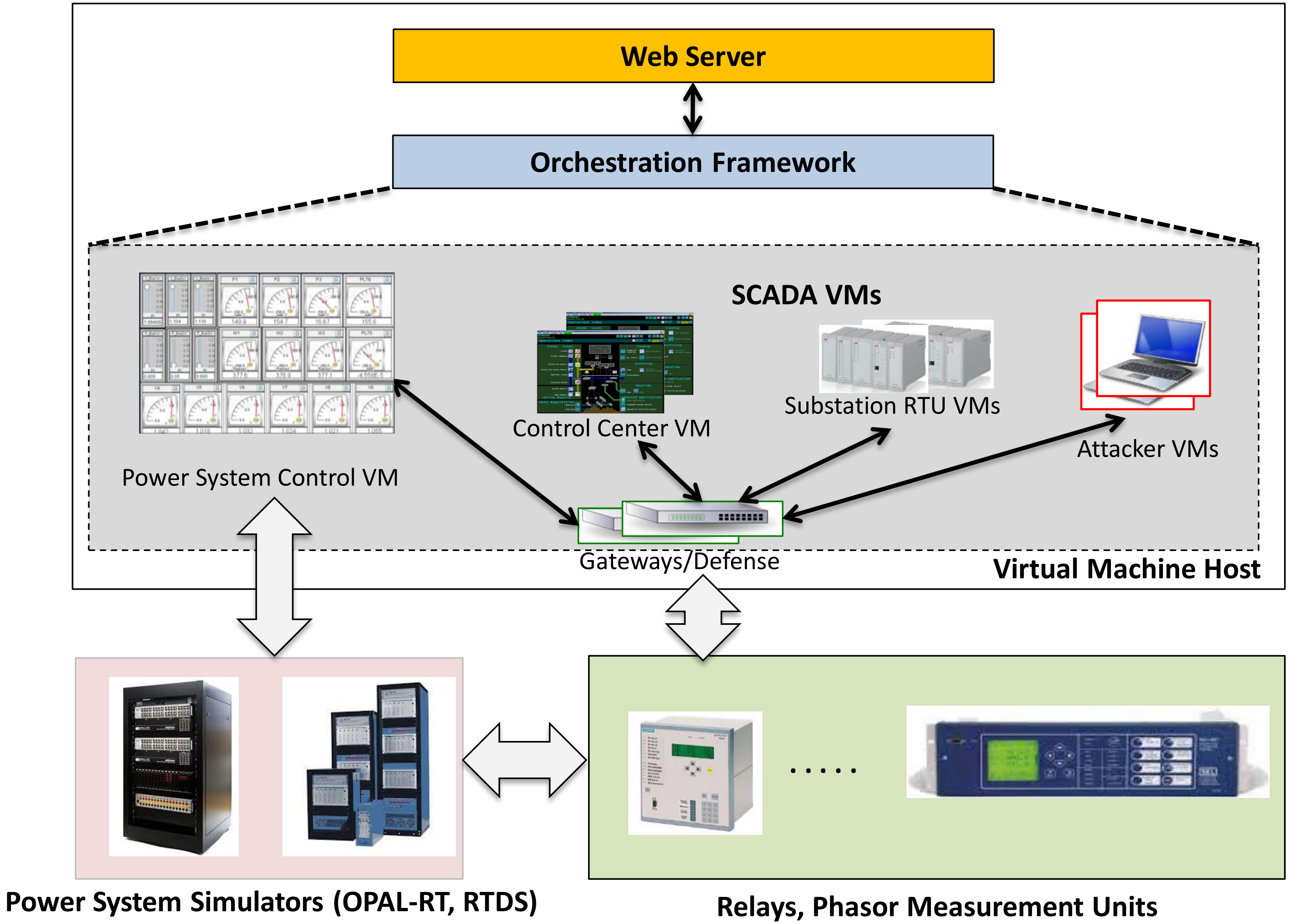


Adam Hahn, Aditya Ashok, Siddharth Sridhar, Manimaran Govindarasu, *Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid,* IEEE Transactions on Smart Grid, vol 4, no. 2, June 2013.

Testbed - Remote Access Framework



PowerCyber Implementation Architecture



ISU *PowerCyber* Testbed - Features

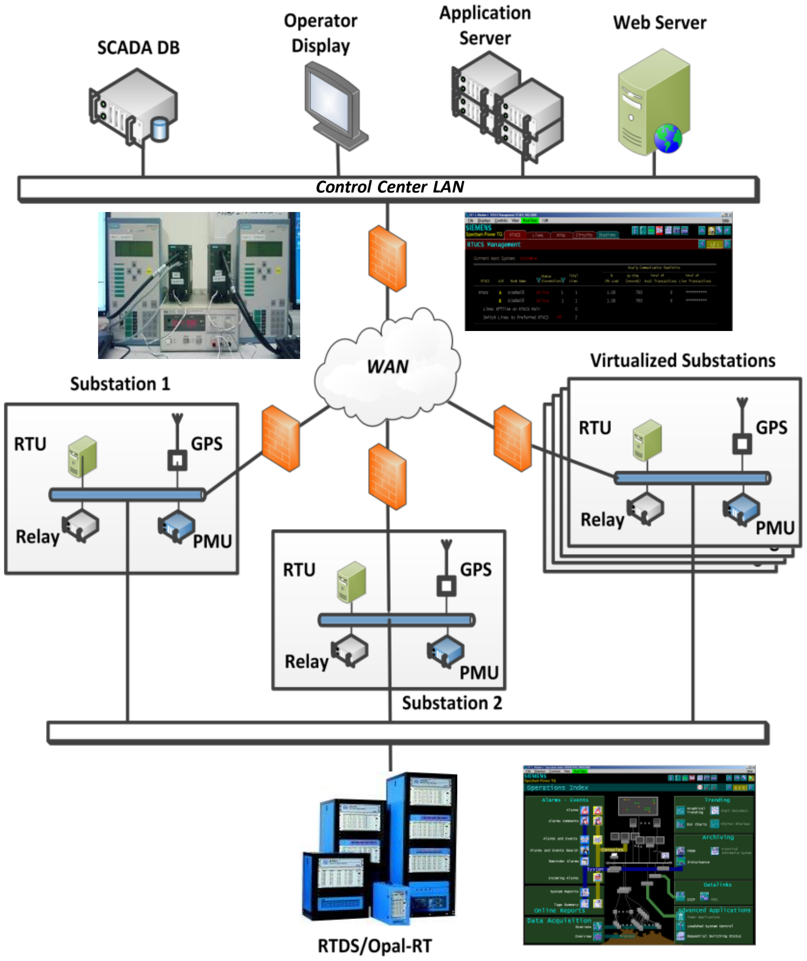
Capabilities

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

Salient Features

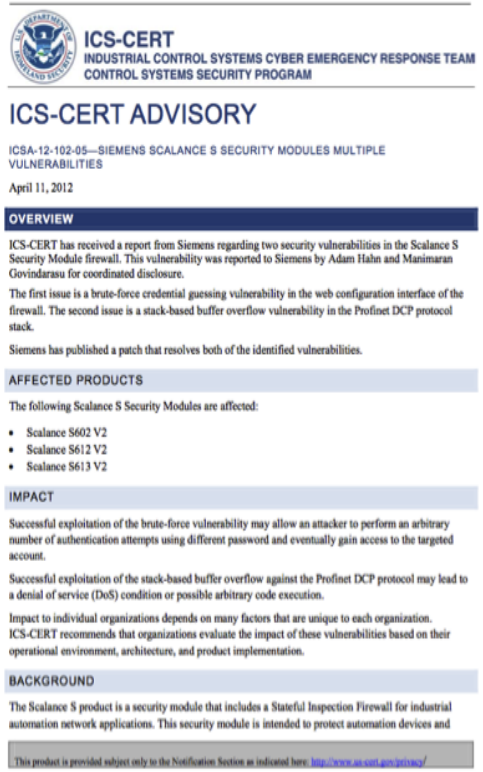
1. ***Cyber-in-the-Loop Real-Time Simulatio****n environment modeling bulk power system.*
2. ***Scalability:***
   - RTDS/Opal-RT provide ability to simulate large power systems with control and protection functions in real-time.
   - Multi-area, substation architecture enabled through virtualization.
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



Testbed Use-Cases: 1, 2, 3

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.

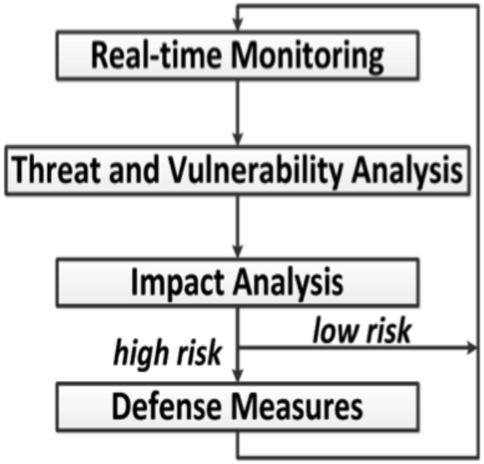
BACKGROUND

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/

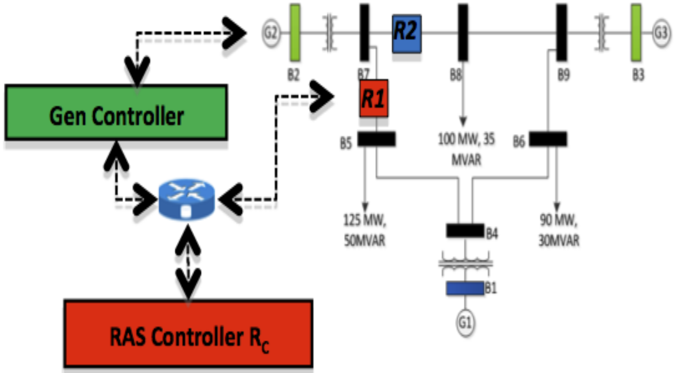
Risk Assessment and Mitigation

- 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

Sample Story Board Scenarios – Attacks

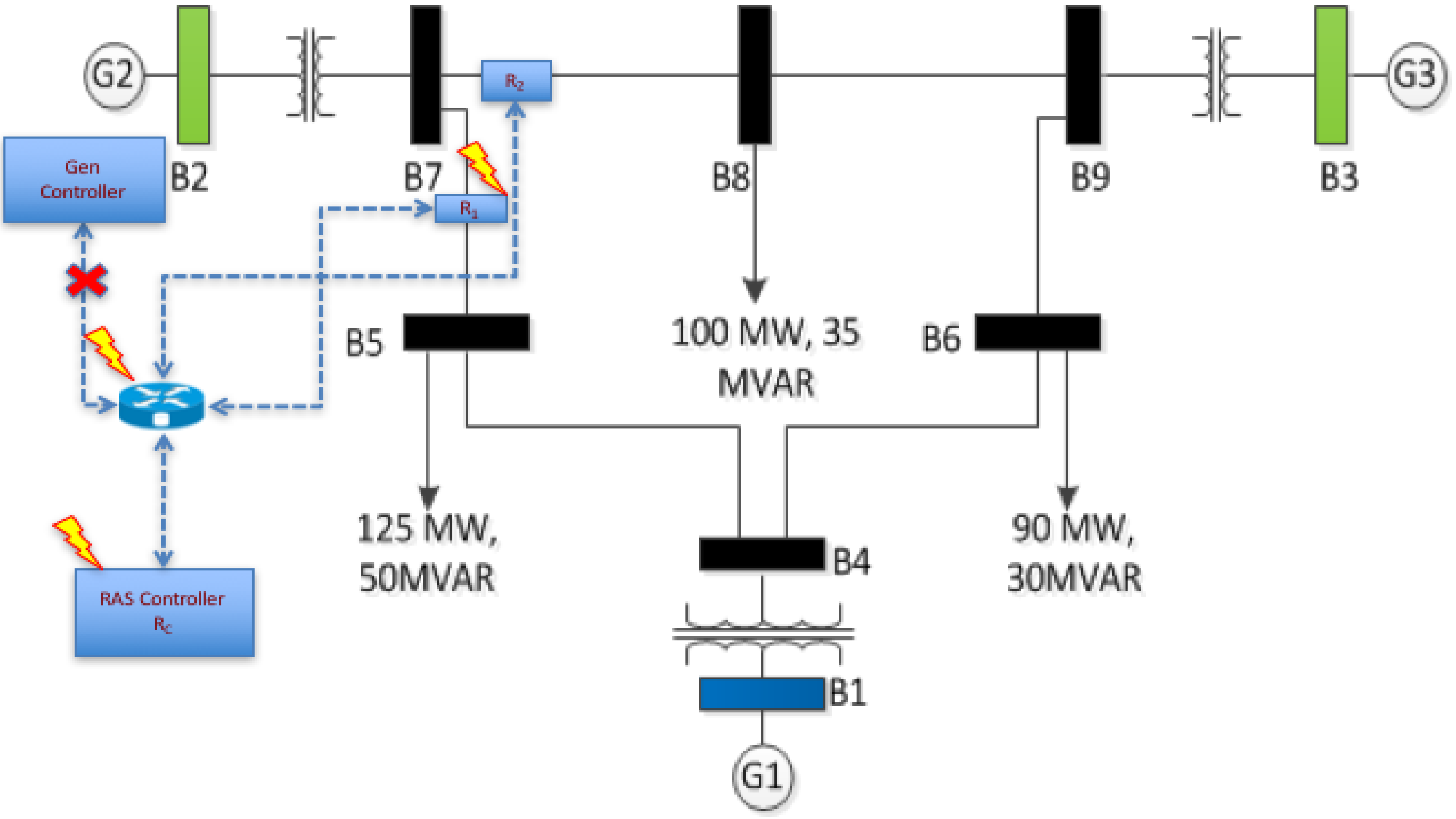
#	Storyboard Description	Attack Vectors
✓ 1	Cascading outage through a coordinated attack on power system protection scheme	Command injection attack to trip relay DoS attack to disrupt protection scheme
✓ 2	Manipulating AGC measurements/controls to affect system frequency	ARP spoofing to intercept communication MITM attack to modify measurements
❑ 3	Manipulating SCADA measurements to affect situational awareness in State Estimator	ARP spoofing to intercept communication MITM attack to spoof measurements
✓ 4	Using unencrypted RTU communication to send arbitrary commands to trip breakers	Command injection attack to send trip commands to relays
✓ 5	Denial of Service attack on RTU/protection devices communication to blind SCADA	DoS attack targeting RTU/ relays targeting specific ports
✓ 6	Exploiting Social Engineering to gain access to Energy Management Systems	Phishing attack to download, install malicious code Reverse shell, VNC to exploit access to EMS
❑ 7	Manipulating protection settings using Substation Automation tools	Phishing attack to install malicious code Program relays to rogue configurations

Sample Story Board Scenarios – Defenses

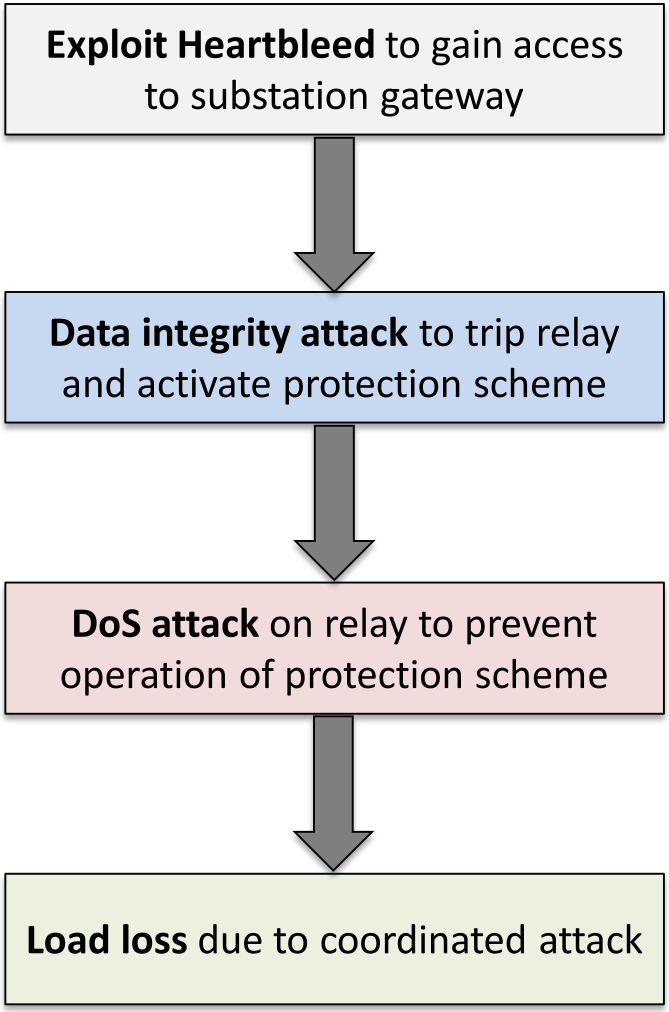
#	Storyboard Description	Defense Measures
✓ 1	Cascading outage through a coordinated attack on power system protection scheme	• Cyber ✓ Firewalls • IDS/IPS ✓ Moving Target Defense ✓ Patch management ✓ VPN – encryption ✓ 2-factor authentication • Cyber-Physical ✓ Domain specific anomaly detection ✓ Model-based mitigation
✓ 2	Manipulating AGC measurements/controls to affect system frequency	
□ 3	Manipulating SCADA measurements to affect situational awareness in State Estimator	
✓ 4	Using unencrypted RTU communication to send arbitrary commands to trip breakers	
✓ 5	Denial of Service attack on RTU/protection devices communication to blind SCADA	
✓ 6	Exploiting Social Engineering to gain access to Energy Management Systems	
□ 7	Manipulating protection settings using Substation Automation tools	

Storyboard (CPS-SEC) – RAS attack-defense

IEEE 9 bus system with Remedial Action Scheme (RAS)



Storyboard – AGC attack-defense

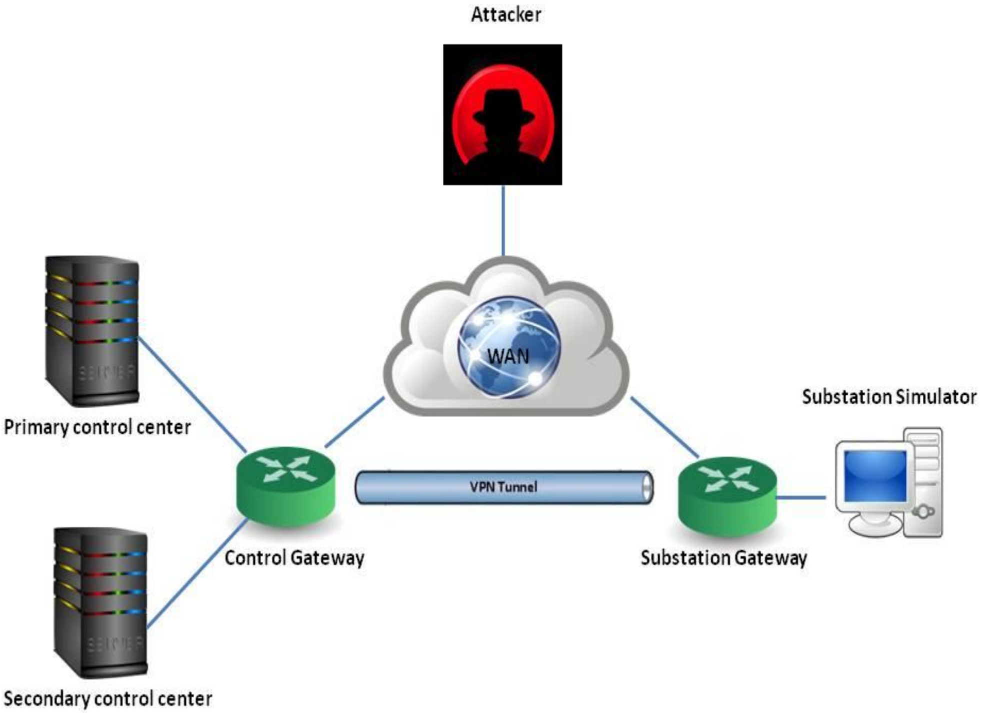


Exploit Heartbleed to gain access to substation gateway

Data integrity attack to trip relay and activate protection scheme

DoS attack on relay to prevent operation of protection scheme

Load loss due to coordinated attack



- ✓ **Patch management**
- ✓ **Firewall rules**
- ✓ **Moving Target Defense**

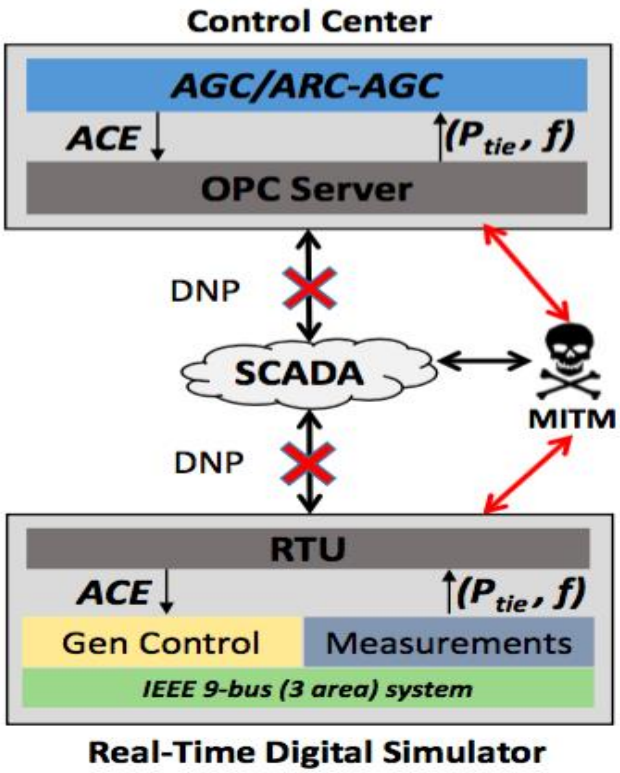
Story Board (CPS-SEC) – AGC Security

ARP spoofing attack intercepts communication between RTU and control center

MITM attack modifies tie-line power flow and frequency measurements to AGC

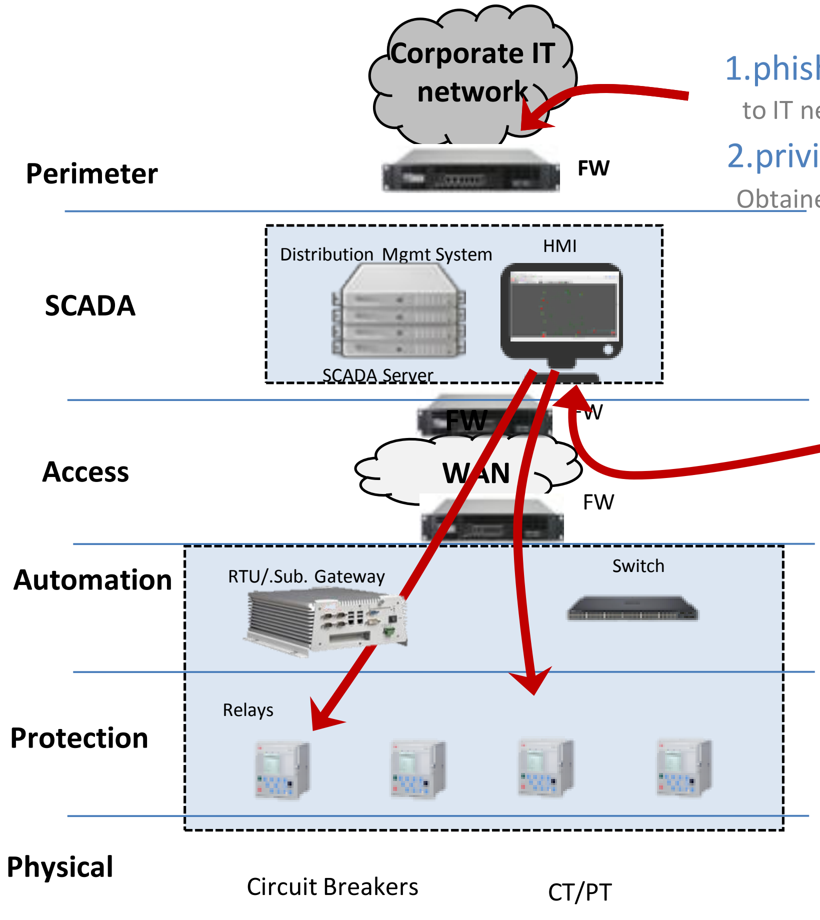
Scaling/ramp attacks on tie-line power flow and frequency measurements lead to frequency drop

Sustained frequency drop leads to **load shedding**



Domain-specific anomaly detection
Model-based mitigation

Ukraine grid’s attack in Dec. 2015 (revisited)



IT

1.phishing email

to IT network

2.privilege escalation

Obtained admin on DC

OT Pre-Impact

3.ot vpn login

Stolen credential from DC used to remotely login to vpn

4.install malware

BlackEnergy malware installed on control systems

5.remote hmi session

Created remote operators session to SCADA server

6.trip breakers

Operate key circuit breakers, 225,000 customers offline

OT Post-Impact

7.disable systems

Wipe SCADA servers, brick serial-ethernet converts and control center ups

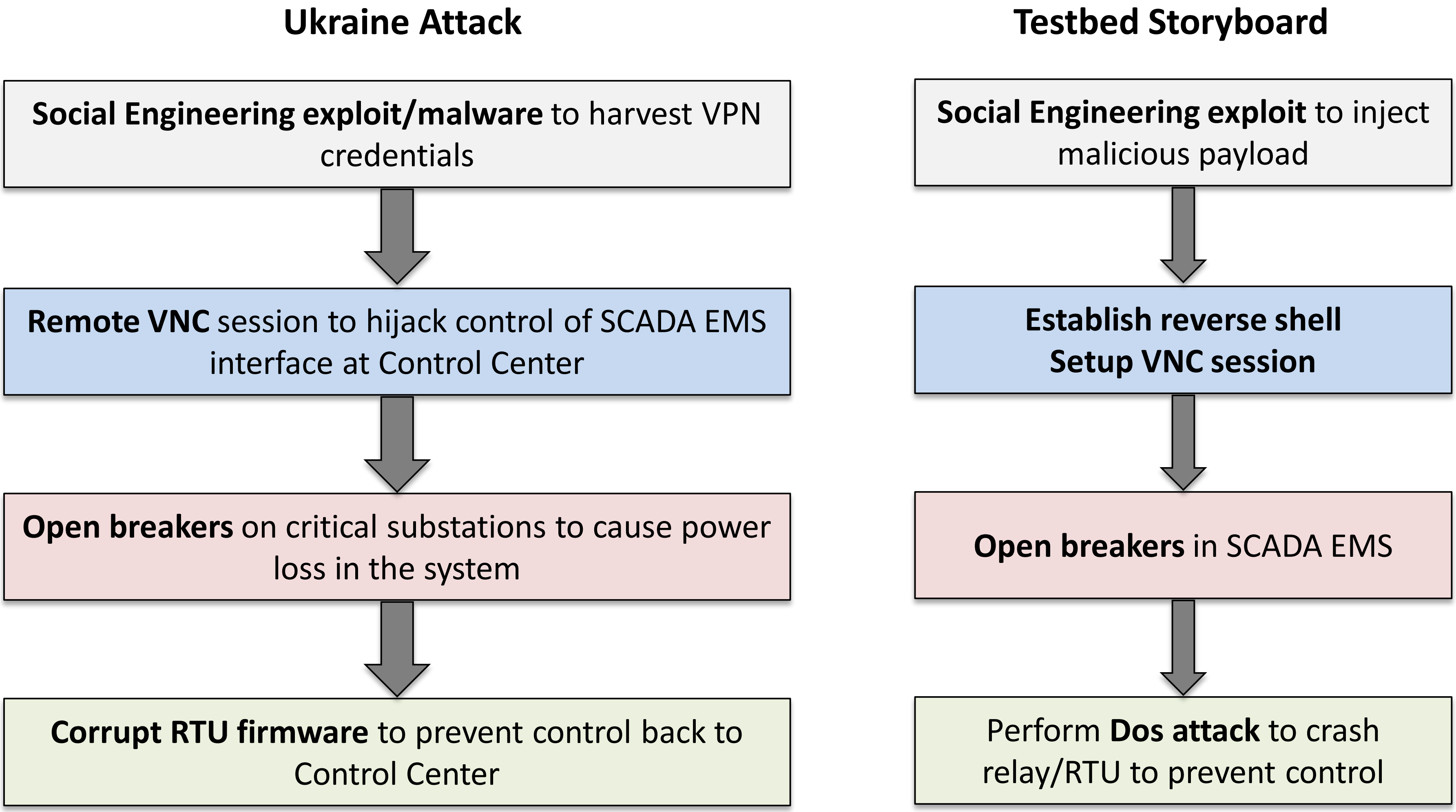
8.telephone ddos

Telephone DDoS prevents communication about grid state

225K customers without power

Ack: Dr. Adam Hahn, Washington State University

Ukraine Attack 2015 modeled in *PoweCyber* testbed



Ukraine Attack

Social Engineering exploit/malware to harvest VPN credentials

Remote VNC session to hijack control of SCADA EMS interface at Control Center

Open breakers on critical substations to cause power loss in the system

Corrupt RTU firmware to prevent control back to Control Center

Testbed Storyboard

Social Engineering exploit to inject malicious payload

Establish reverse shell
Setup VNC session

Open breakers in SCADA EMS

Perform **Dos attack** to crash relay/RTU to prevent control

Defense for Ukraine attack 2015

Ukraine Attack
Recommended Defense measures

Security awareness & training

Network Monitoring – SIEM, IDS
Application Firewalls

VPN: 2-factor authentication,
time of use access

Disable remote access and
management of field devices

Testbed Storyboard
Defense measures

Firewall: Egress Filtering

□ VPN: 2-factor authentication

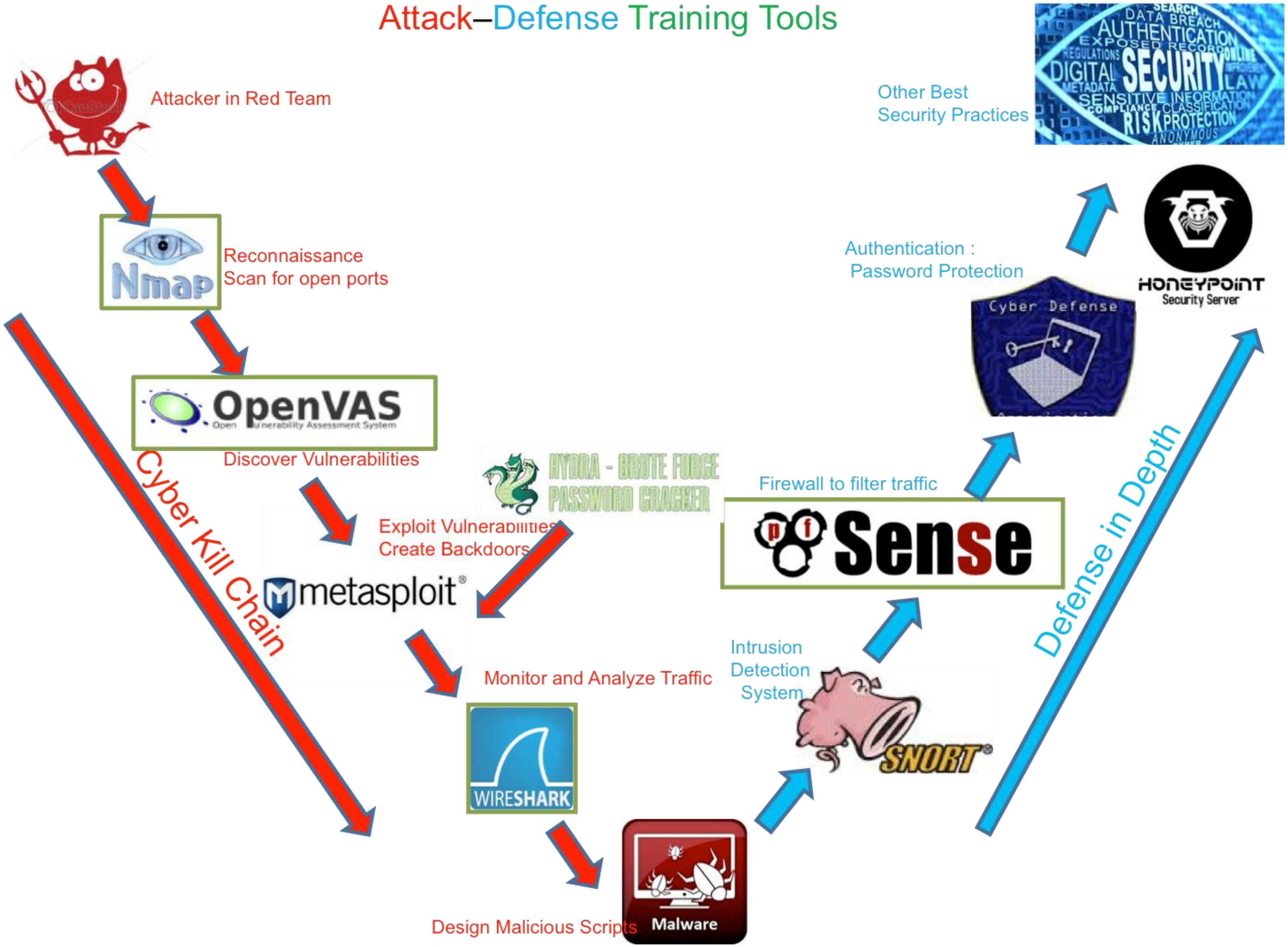
□ Network monitoring – IDS/IPS

□ SIEM – Logging and event correlation

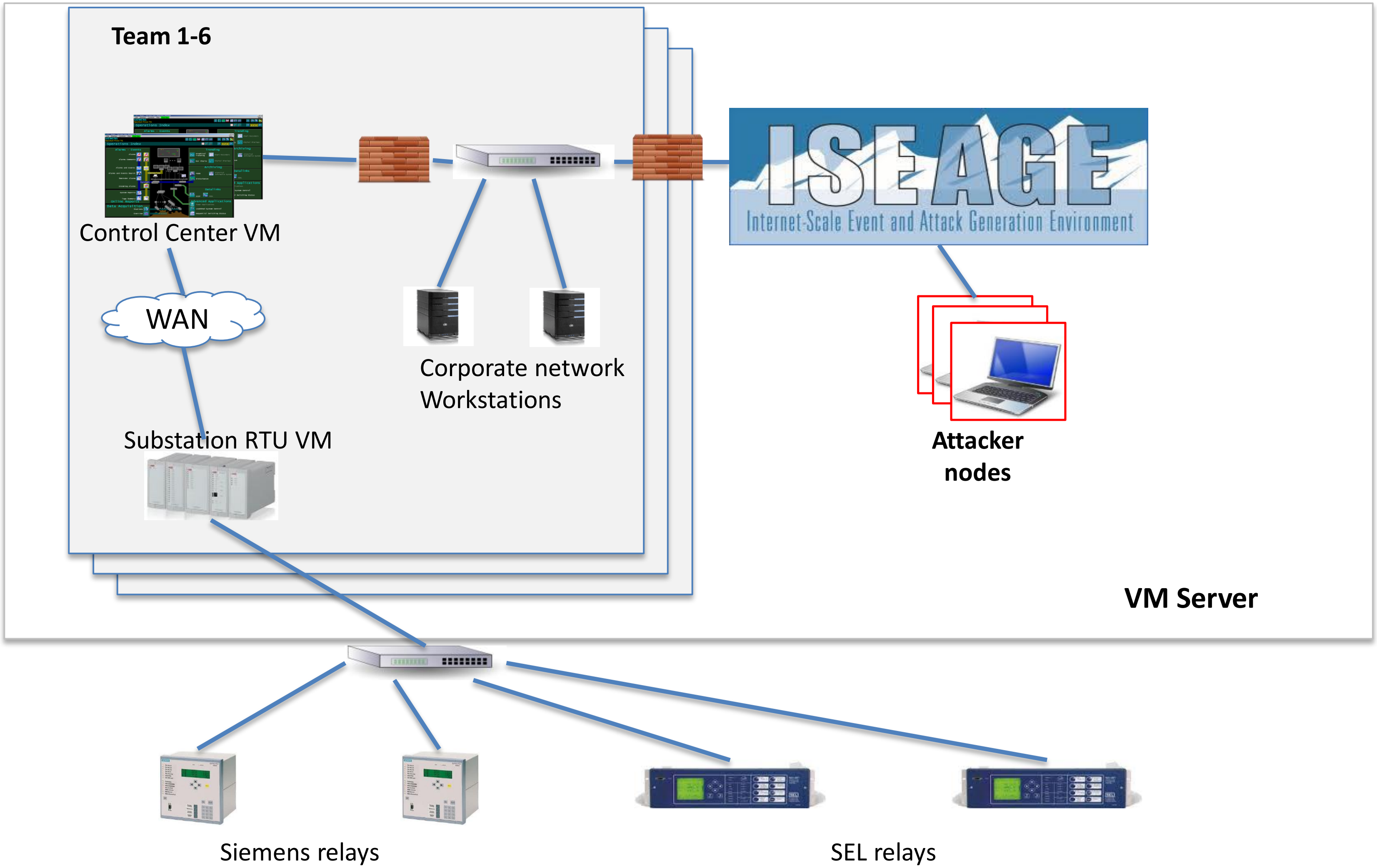
Outline of **Module 6**

- Testbed Concepts & Architecture
- Case Study – Iowa State's *PoweCyber Security*
- *Case Study* – IIT Bombay's *WAMS Testbed (Demo)*
- Testbed R&D needs
- Testbed Demos

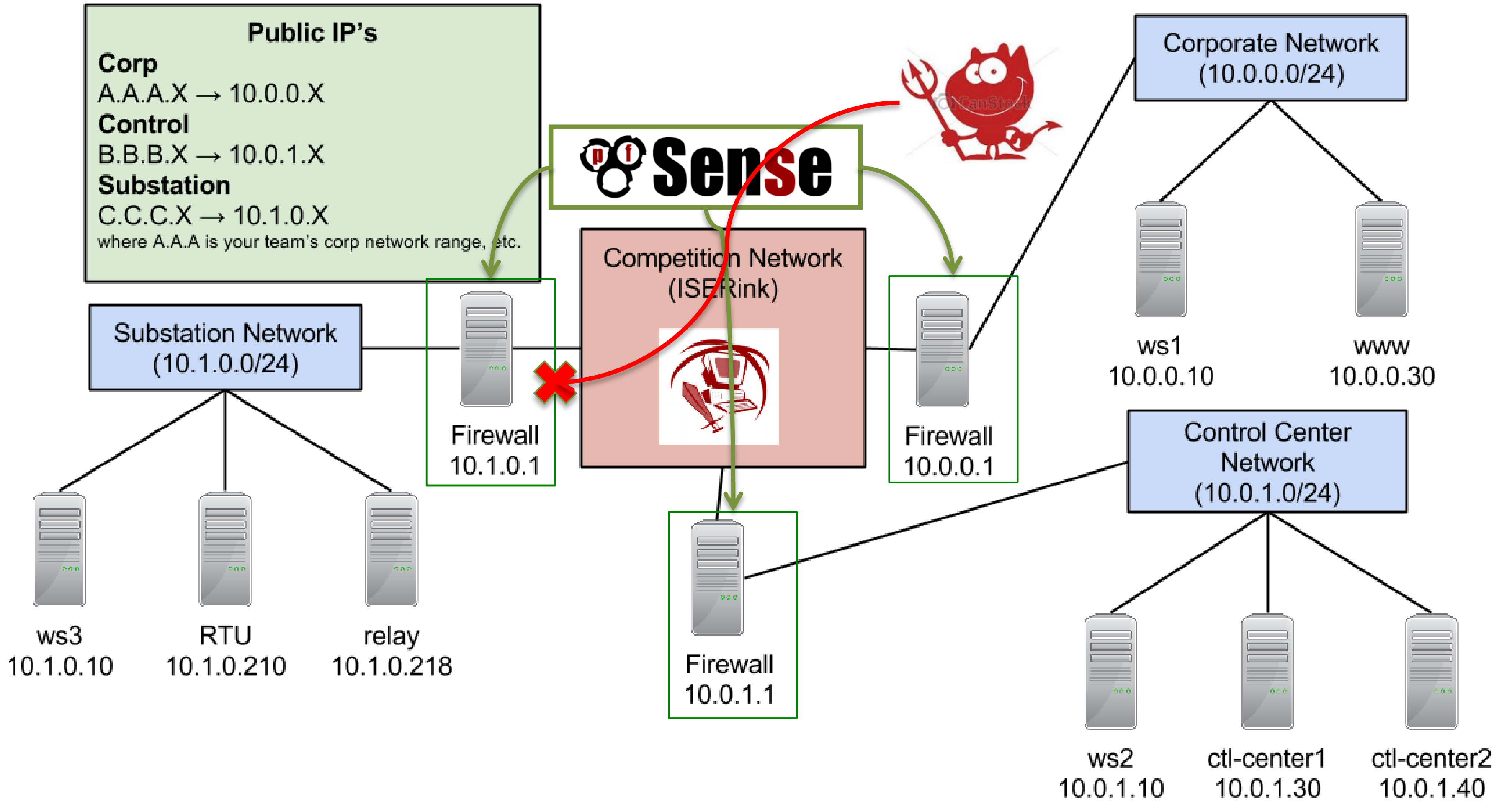
Use-Case 4: Cybersecurity Training Framework (Attacks-Defenses)



Training Environment – An instance of SCADA for each team



Testbed for Attack-Defense Training (an instance)



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.

pfSense

Competition Network (ISERink)

Substation Network (10.1.0.0/24)

Firewall 10.1.0.1

Firewall 10.0.0.1

Firewall 10.0.1.1

Corporate Network (10.0.0.0/24)

Control Center Network (10.0.1.0/24)

ws3 10.1.0.10

RTU 10.1.0.210

relay 10.1.0.218

ws1 10.0.0.10

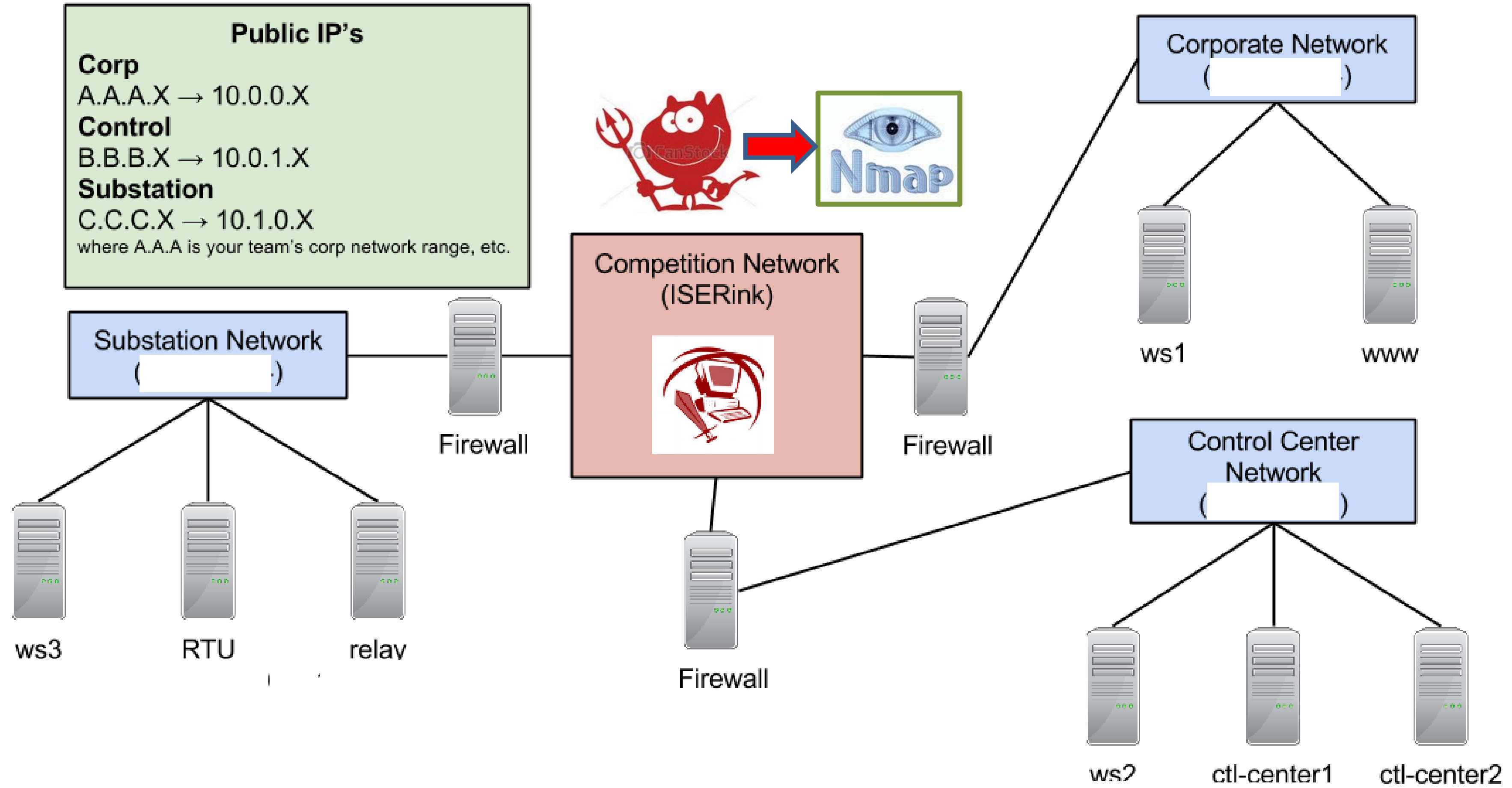
www 10.0.0.30

ws2 10.0.1.10

ctl-center1 10.0.1.30

ctl-center2 10.0.1.40

Before Port Scanning



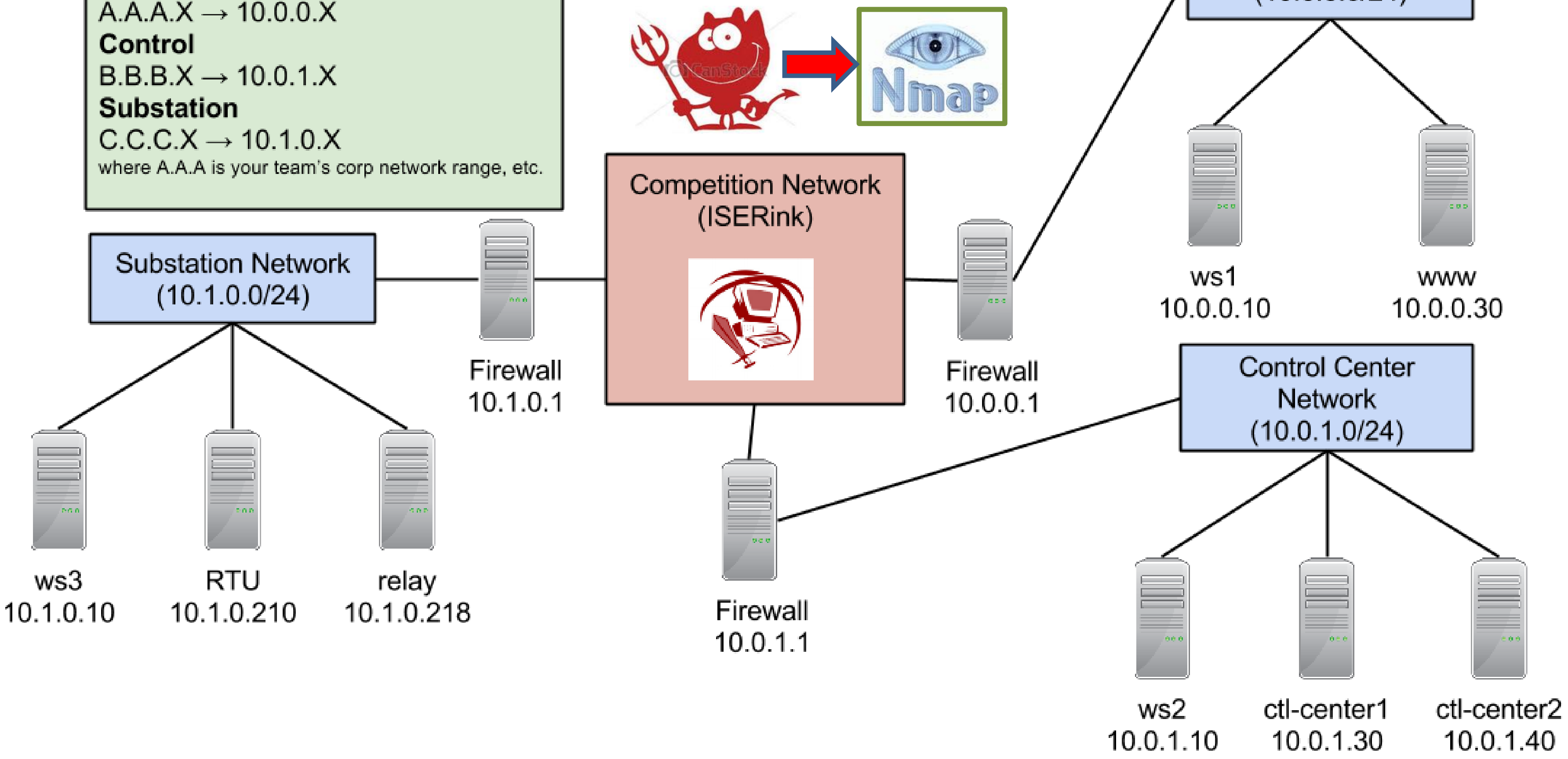
Public IP's

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.

After Port Scanning (Reconnaissance)

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.



Nmap

Competition Network
(ISERink)

Substation Network
(10.1.0.0/24)

Firewall
10.1.0.1

ws3
10.1.0.10

RTU
10.1.0.210

relay
10.1.0.218

Firewall
10.0.1.1

Firewall
10.0.0.1

Corporate Network
(10.0.0.0/24)

ws1
10.0.0.10

www
10.0.0.30

Control Center
Network
(10.0.1.0/24)

ws2
10.0.1.10

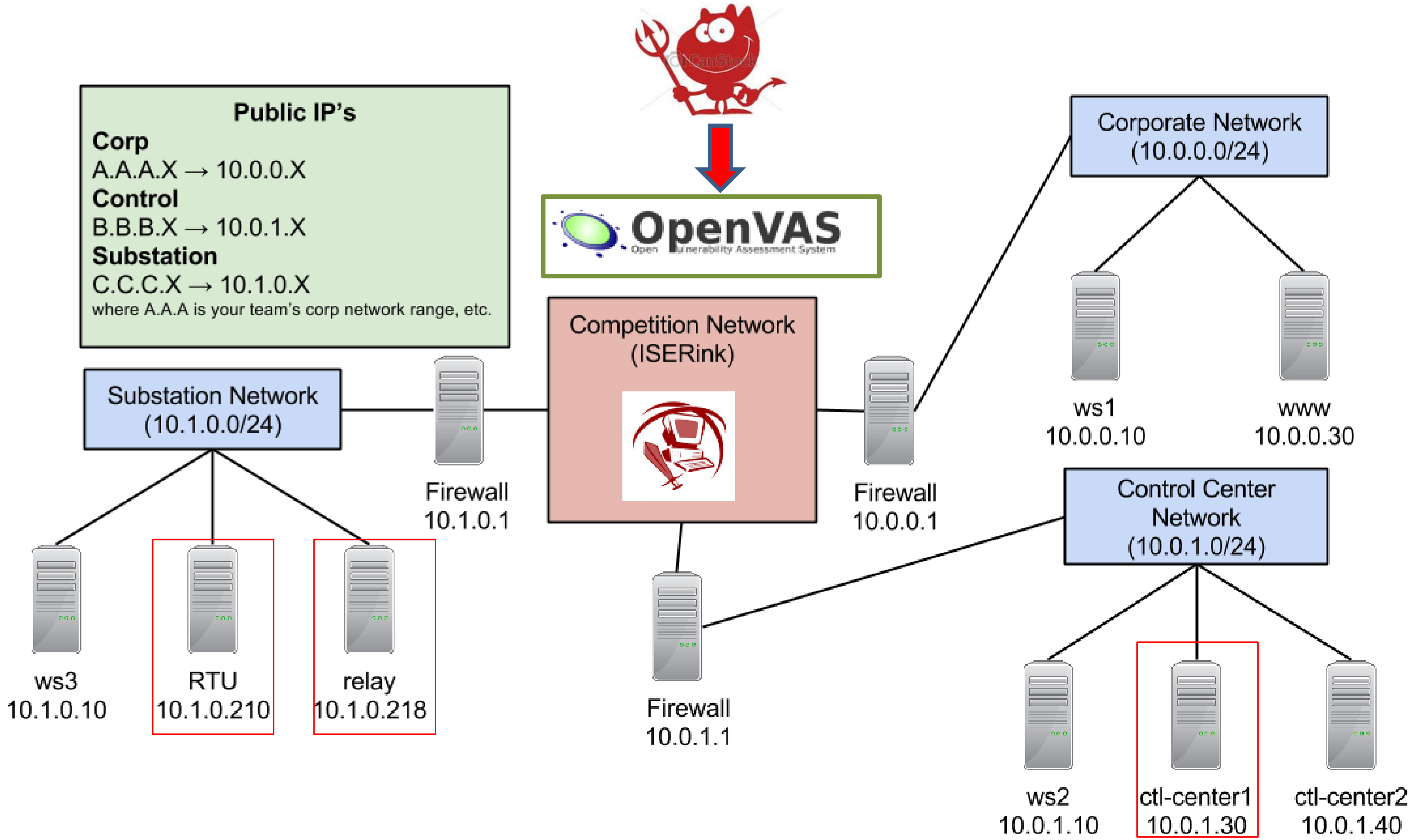
ctl-center1
10.0.1.30

ctl-center2
10.0.1.40

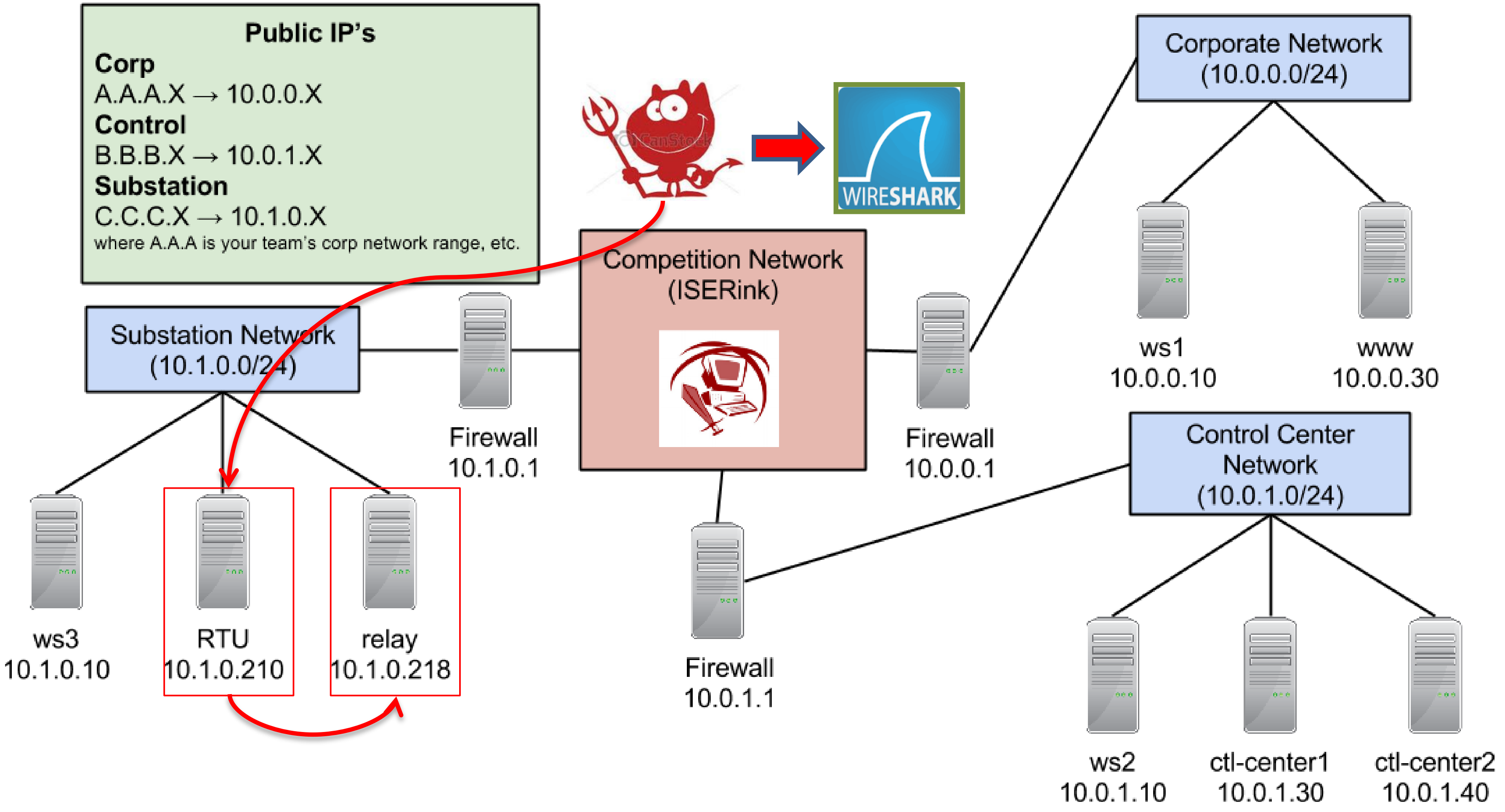
Vulnerability Assessment

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.



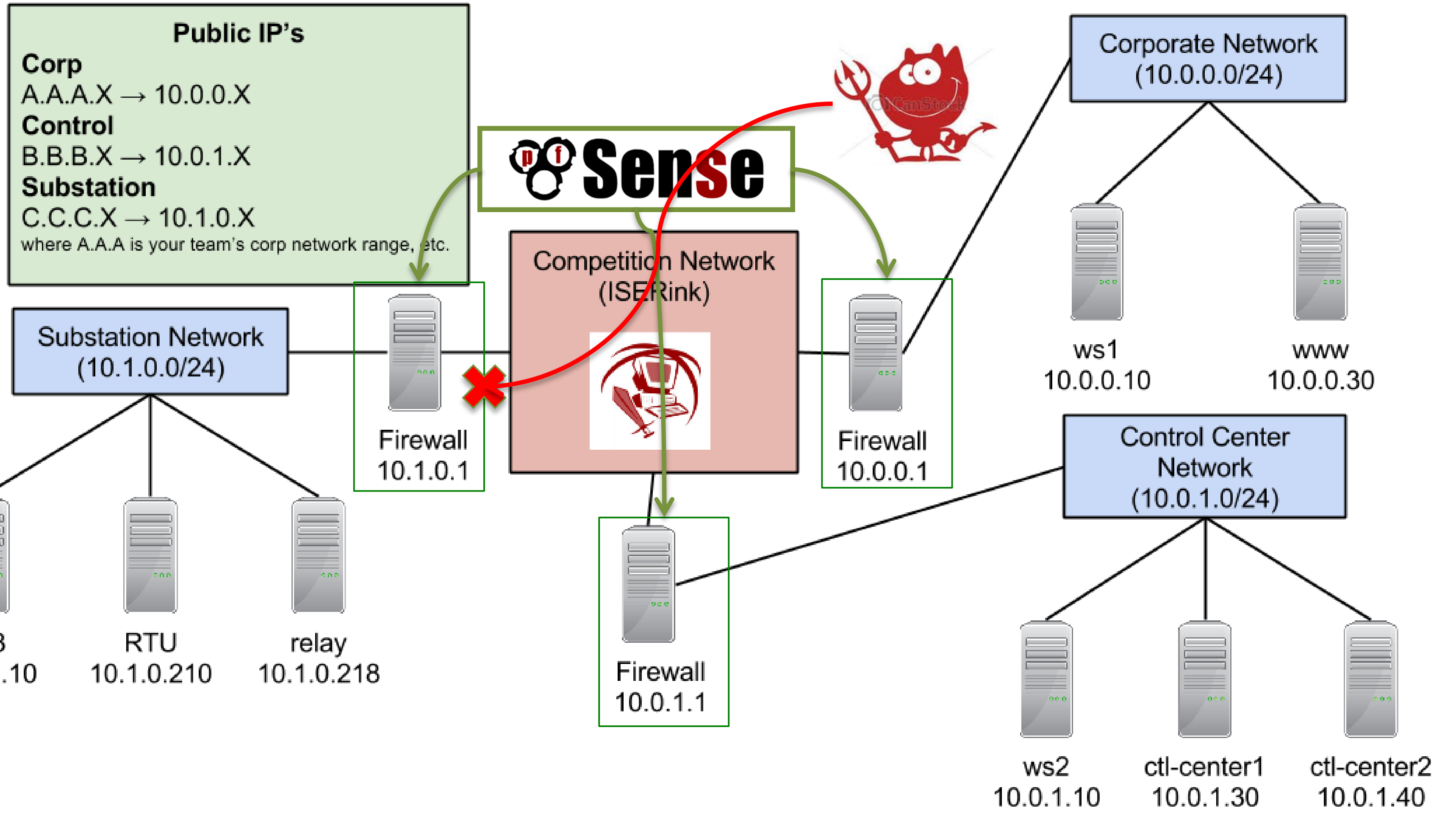
WireShark and Trip Script (Exploitation)



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.

Setting up PFSense (Firewall config)



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.

pfSense

Competition Network (ISERink)

Substation Network (10.1.0.0/24)

Firewall 10.1.0.1

Firewall 10.0.0.1

Firewall 10.0.1.1

Corporate Network (10.0.0.0/24)

ws1 10.0.0.10

www 10.0.0.30

Control Center Network (10.0.1.0/24)

ws3 10.1.0.10

RTU 10.1.0.210

relay 10.1.0.218

ws2 10.0.1.10

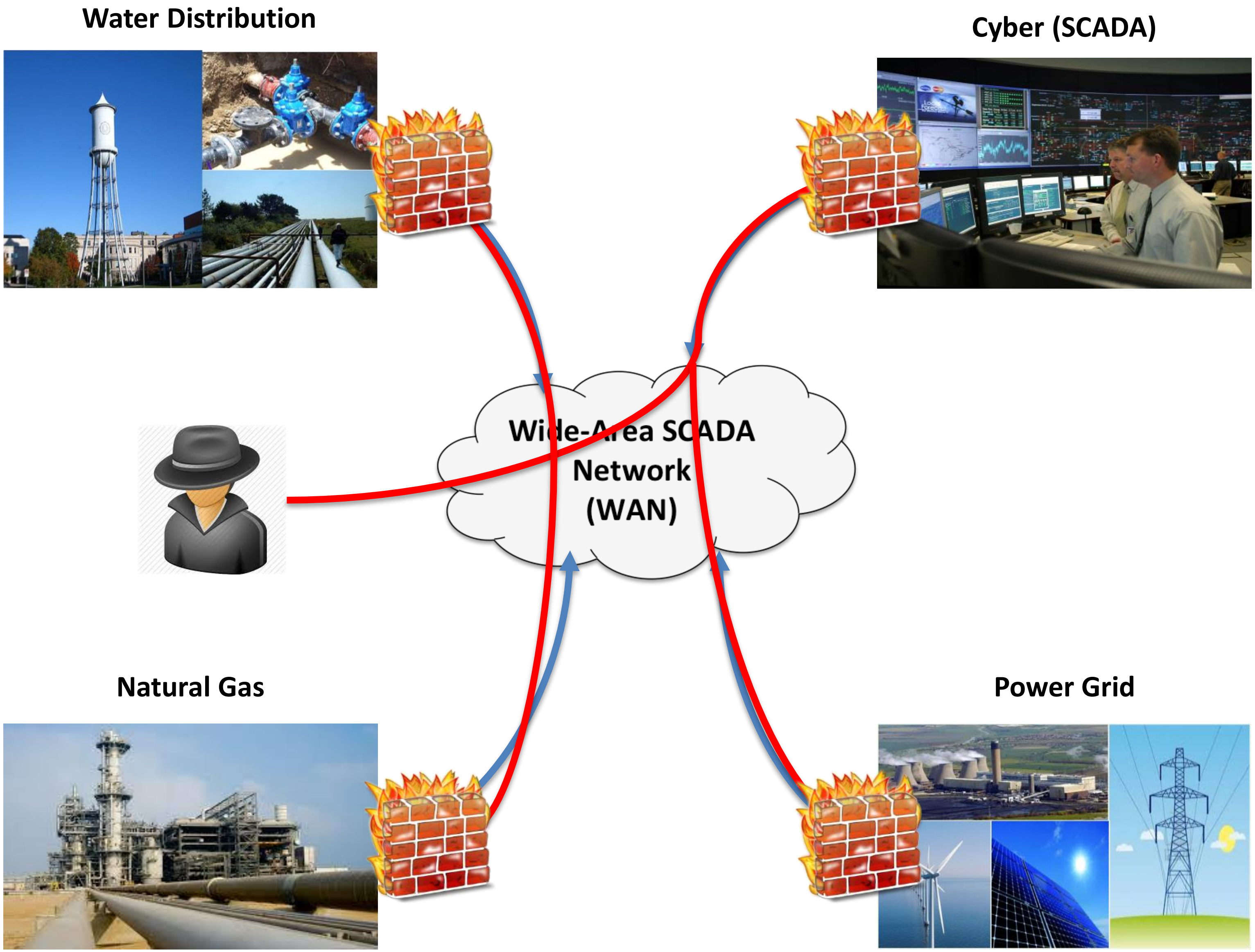
ctl-center1 10.0.1.30

ctl-center2 10.0.1.40

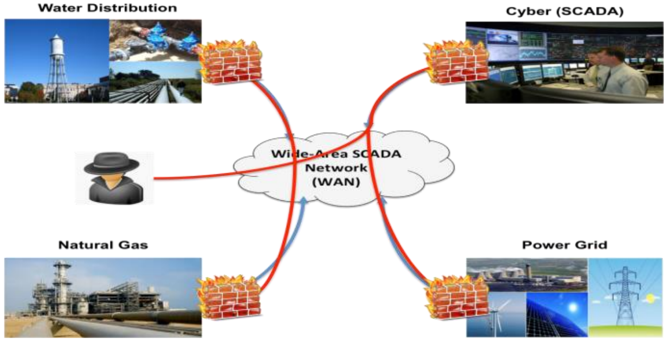
Outline of **Module 6**

- Testbed Concepts & Architecture
- Case Study – Iowa State's *PoweCyber Security*
- *Case Study – IIT Bombay's WAMS Testbed (Demo)*
- Testbed R&D needs
- Testbed Demos

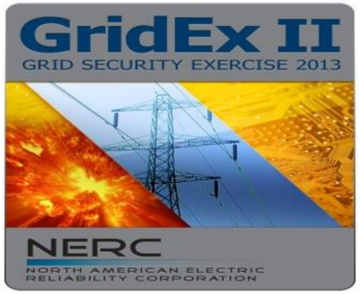
Cyber-Defense Exercise for Critical Infrastructures



CDE: Tabletop → Testbed-based

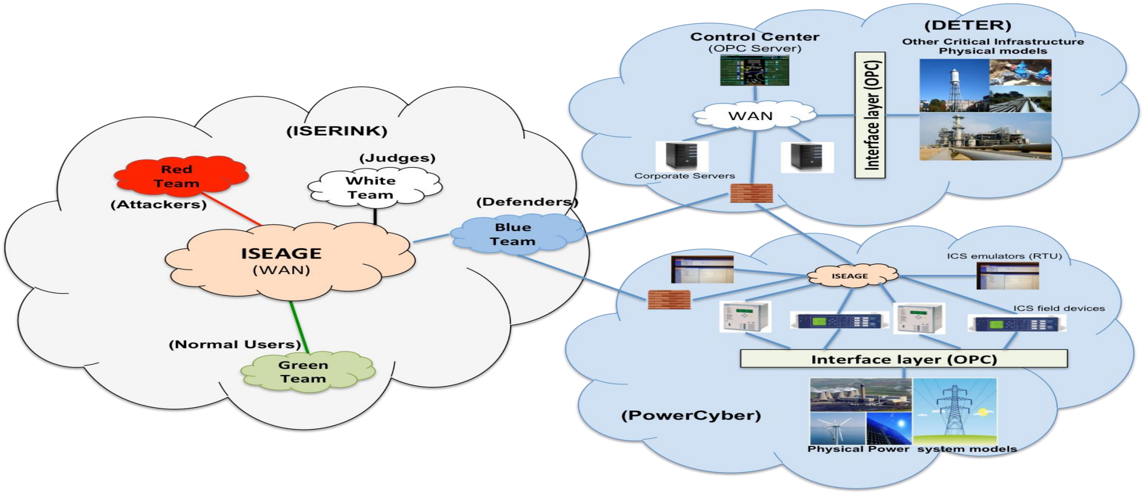


Critical Infrastructure Cyber Security and Cyber Defense


GridEx II
GRID SECURITY EXERCISE 2013
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

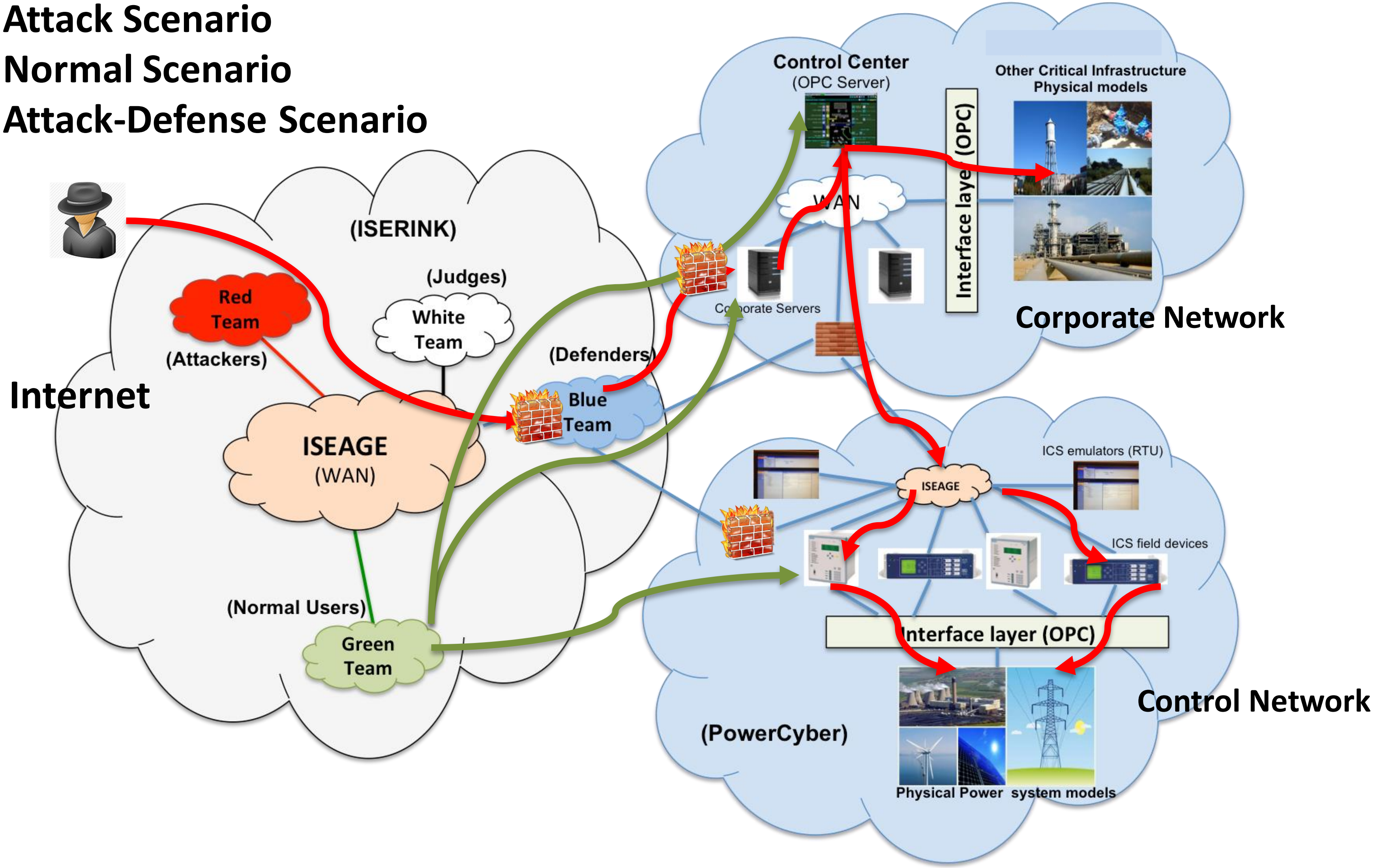


Testbed-based Training Scenarios for Power Grid

Attack Scenario

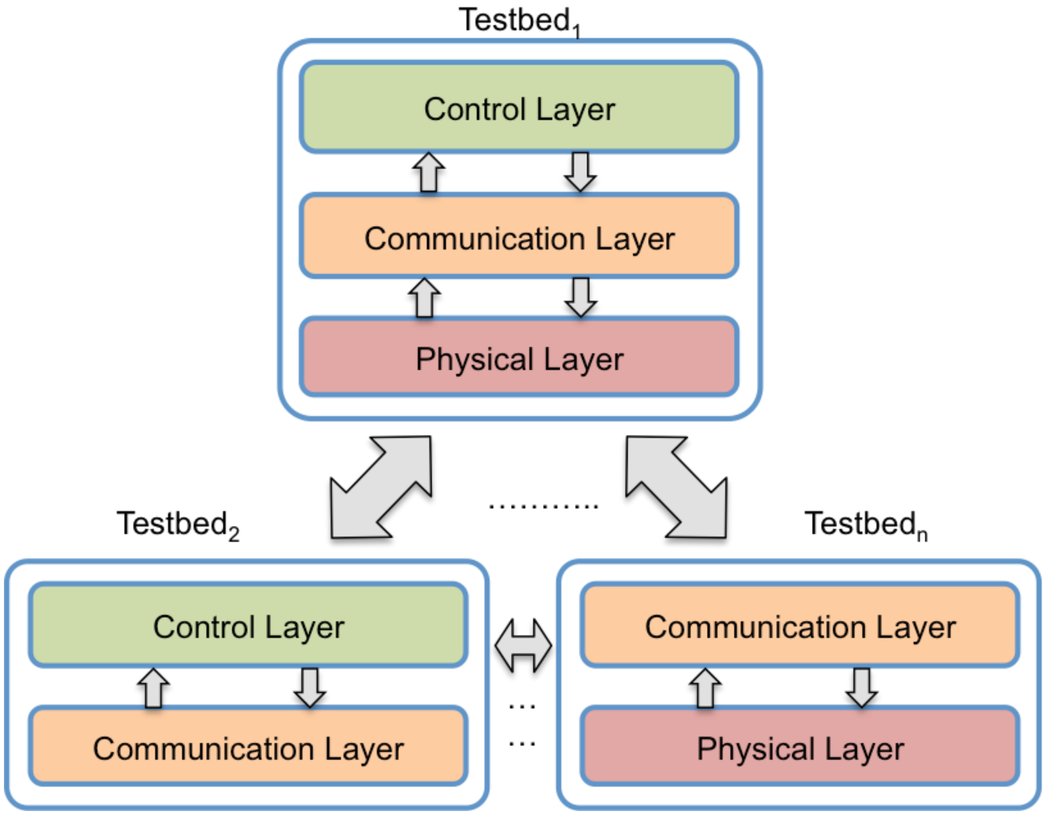
Normal Scenario

Attack-Defense Scenario

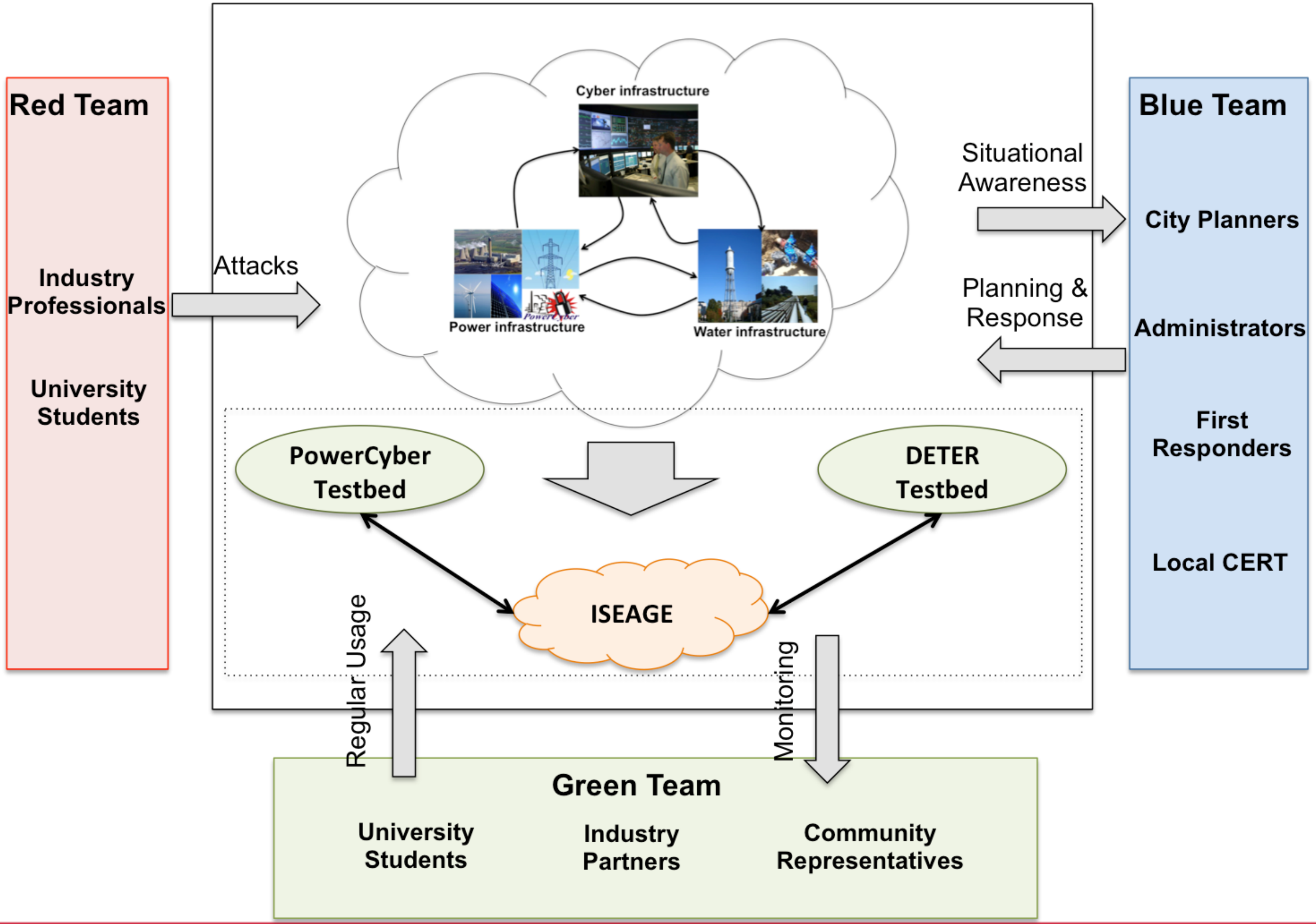


Testbed Federation Concept

- **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.



Testbeds of Interdependent Critical Infrastructures



Red Team

Industry Professionals

University Students

Attacks

Cyber infrastructure

Power infrastructure

Water infrastructure

Situational Awareness

Planning & Response

Blue Team

City Planners

Administrators

First Responders

Local CERT

PowerCyber Testbed

DETER Testbed

ISEAGE

Regular Usage

Monitoring

Green Team

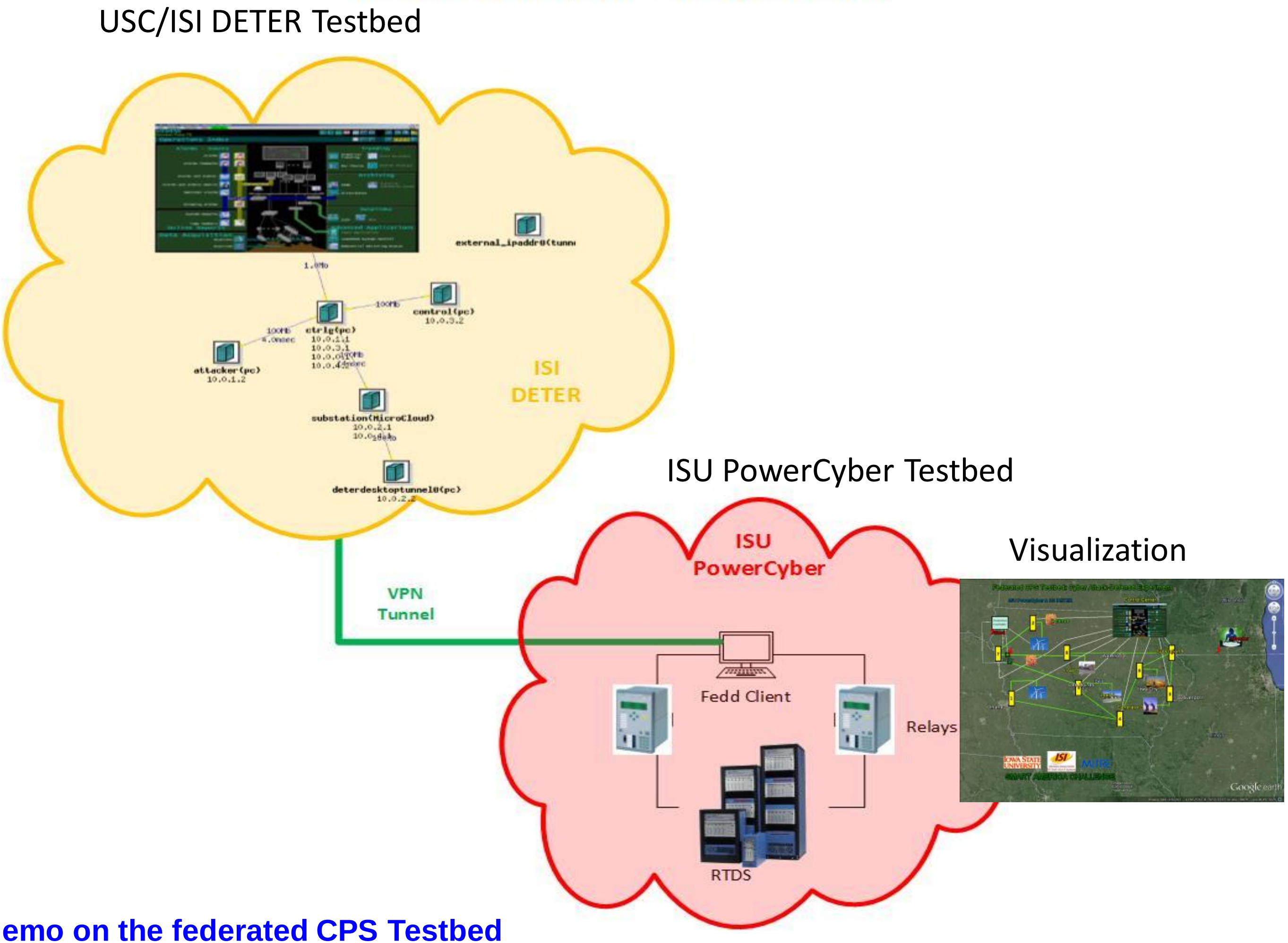
University Students

Industry Partners

Community Representatives

CPS Testbed Federation Architecture

Smart Energy CPS
ISU PowerCyber + ISI DeterLab



[**Attack-defense demo on the federated CPS Testbed**]

Conclusion

- CPS testbeds capture complex interactions between **Cyber-Control-Physic**al subsystems

- Seamless integration of ***Physical, Emulated, Simulated, and Virtual*** components are needed to build a scalable, high-fidelity, cost-effective CPS testbe

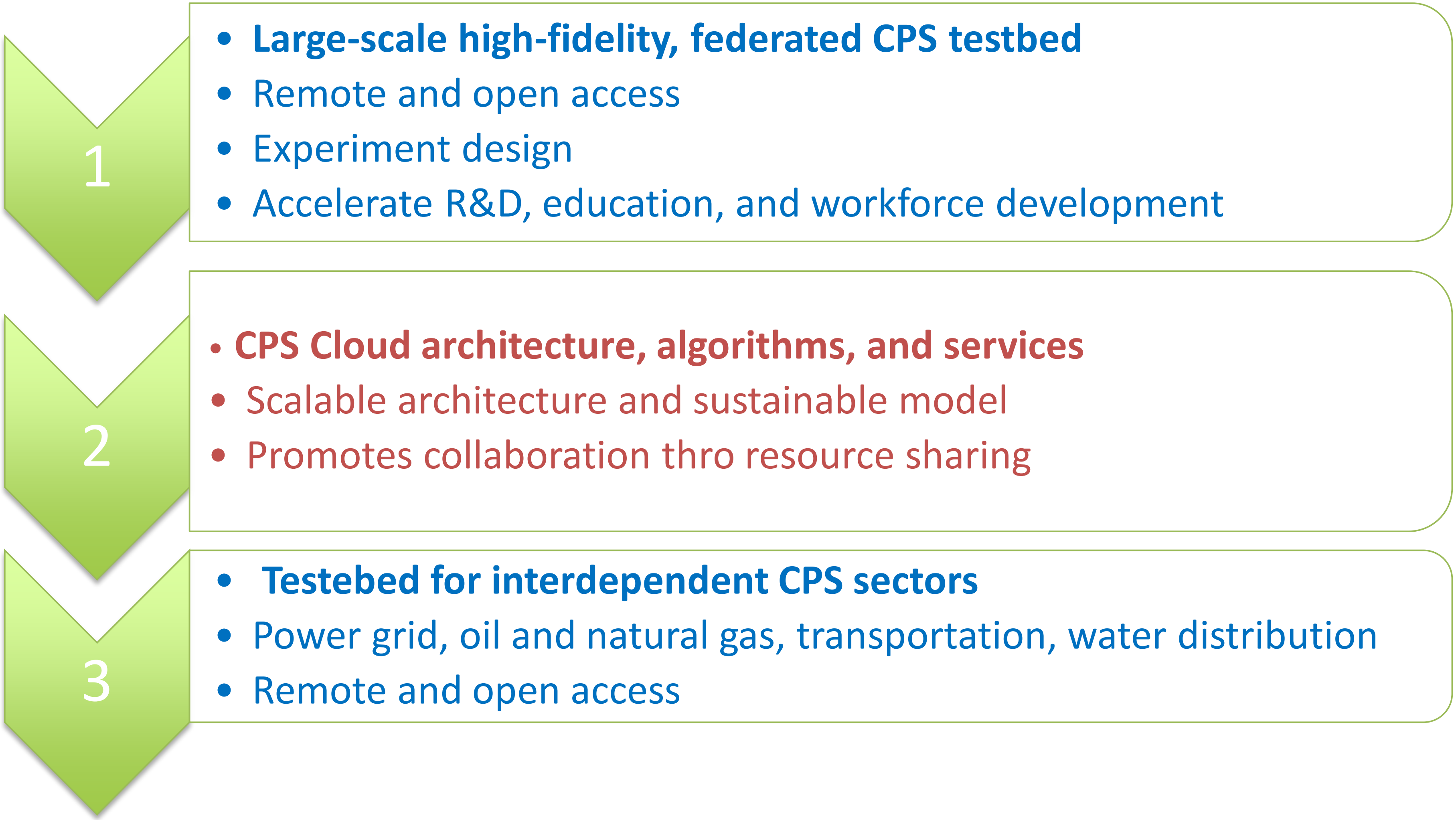
- Testbed based research helps to perform
  - Vulnerability assessment for devices, systems and protocols
  - Impact analysis of cyber events on physical systems
  - Attack-Defense Evaluation and validation

- Testbeds use-cases include **R&D, education, industry training, and cyber defense competitions**

Future Research Opportunities

- Science of Experimentation & Testbed Architectures
- 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

Testbed Demos in ISU’s *PowerCyber* Testbed

- Ukraine 2015 attack – Demo, Q/A