Project Review Presentation – Year 1 (March 7, 2016)

NSF Grant CNS 1446831, jointly funded by NSF and DHS

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

Manimaran Govindarasu (PI)

Venkataramana Ajjarapu (Co-PI)

Doug Jacobson (Co-PI)

Iowa State University

http://powercyber.ece.iastate.edu

Project Tasks & Deliverables

- **End of Year 1**

1. Scale up the power system's real-time simulator to simulate up to ~100-bus system and necessary models development.

2. Development of necessary interfaces between the SCADA system (cyber) and the real-time simulator (physical) to achieve required fidelity.

3. Development and implementation of testbed federation building blocks and proof-of-concept implementation including those for CPS Cyber Defense Competition (CPS-CDC)

4. Develop, document, and demonstrate open Application Programmer Interface and building block for testbed use.

5. Document test-bed initial capabilities including user guide

Project Tasks & Deliverables

- **End of Year 2**

1. Implement and demonstrate exemplar protection and control algorithms in the testbed.

2. Demonstrate remote experimentation capability through interfacing the testbed's front-end to the back-end through automatic scripting. Document the interface.

3. Provide briefing documenting preliminary attack-defense experimentations on the testbed, with testing of remote access capabilities.

4. Host CPS-CDC and disseminate the models and experience to a broader university community

5. Document community outreach activities to grow the research community using test-bed

Project Summary

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

Challenge:

*Developing a low-cost, scalable, high-fidelity testbed that captures cyber and physical system properties, and their interdependencies for conducting realistic cyber security experimentation

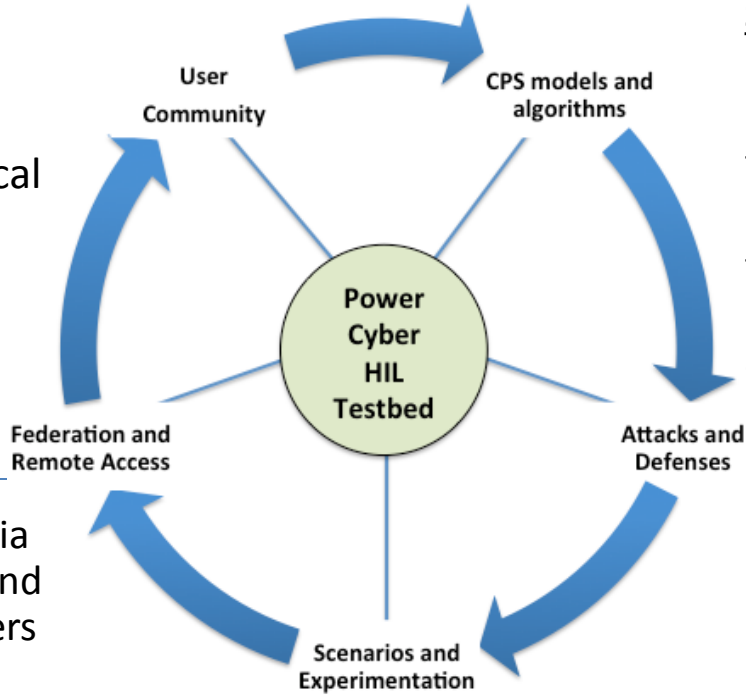
Solution:

*Low-cost: Testbed federation via synergistic leveraging of cyber and physical resources across partners

*Scalability: Virtualization, OPC, abstractions, modules, libraries

*Fidelity: CPS models & algorithms

*Realism: WAMPAC algorithms, Stealthy attacks and defenses



Scientific Impact:

*A novel architecture with abstractions for testbed federation and remote access

*Novel models and algorithms for wide-area monitoring, protection, and control for the smart grid *Experimental results

Broader Impact:

***Research:** Realistic platform to evaluate and validate cyber security and smart grid solutions

***Industrial:** Pilot studies & Cyber security training to engineers and operators of power industry

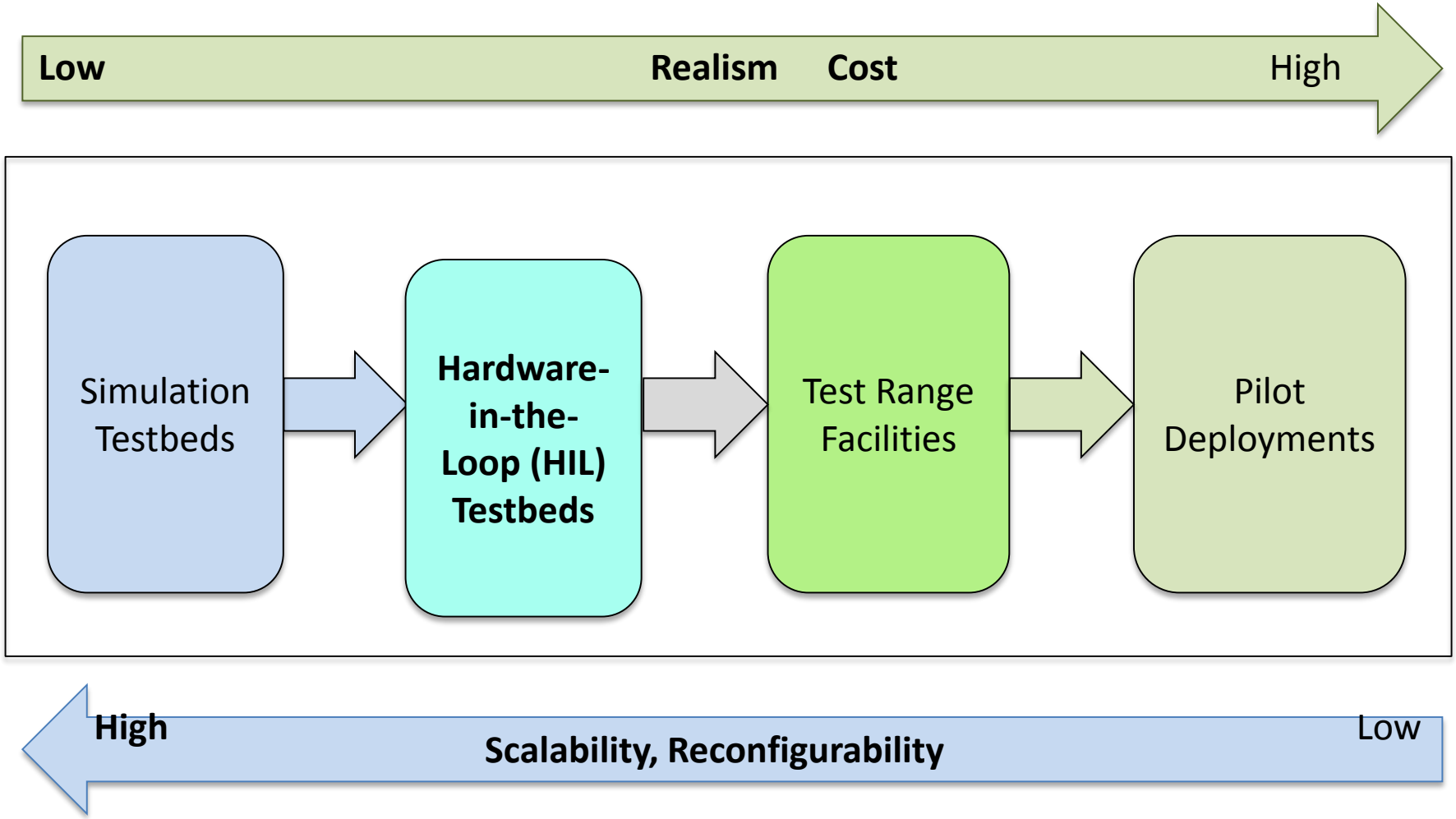
***Education:** Workforce development via cyber security curriculum and cyber defense competitions, and K-12 outreach

Grant CNS 1446831, Iowa State University

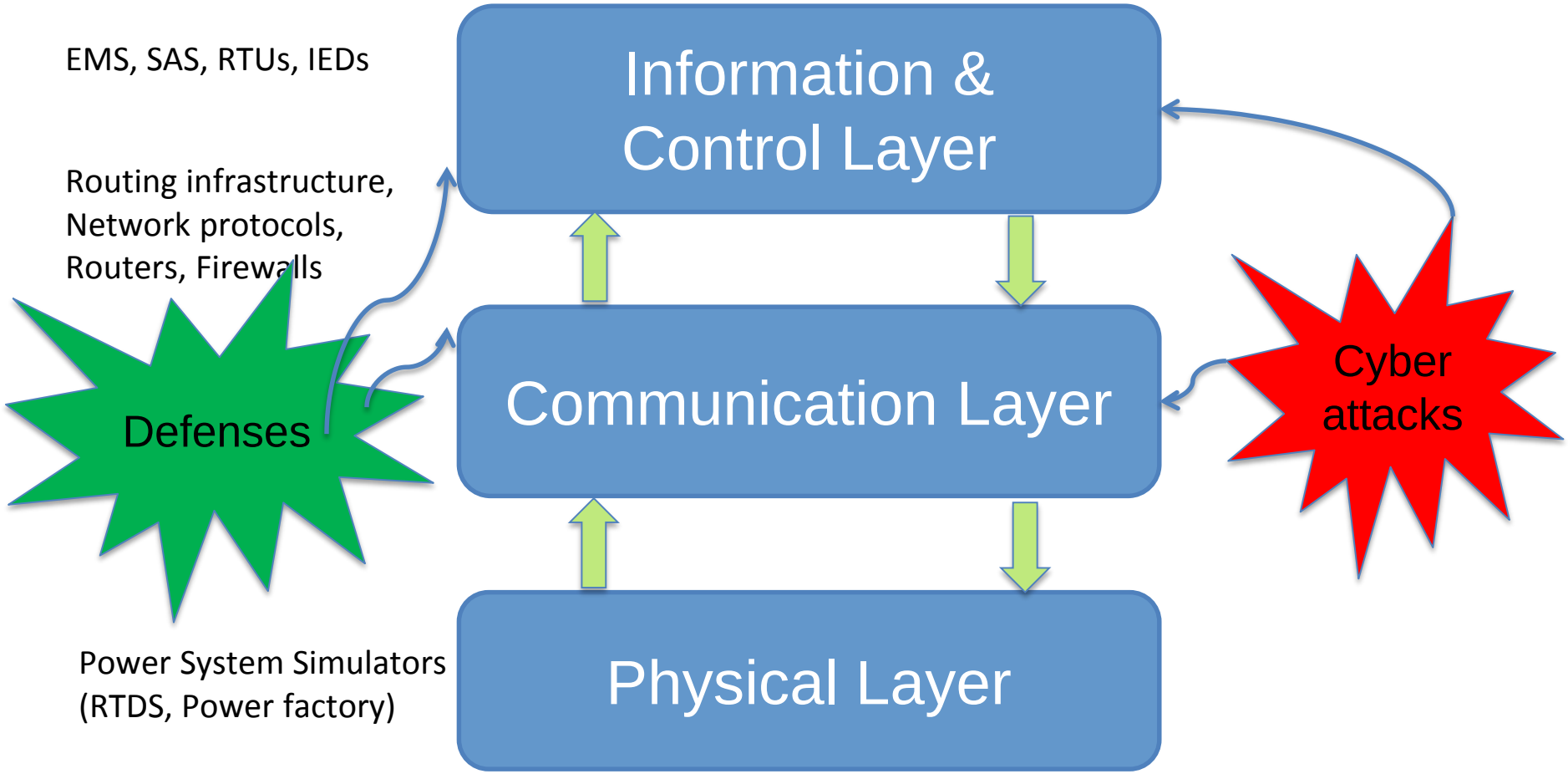
PI: Manimaran Govindarasu

Email: gmani@iastate.edu

CPS Testbeds Spectrum

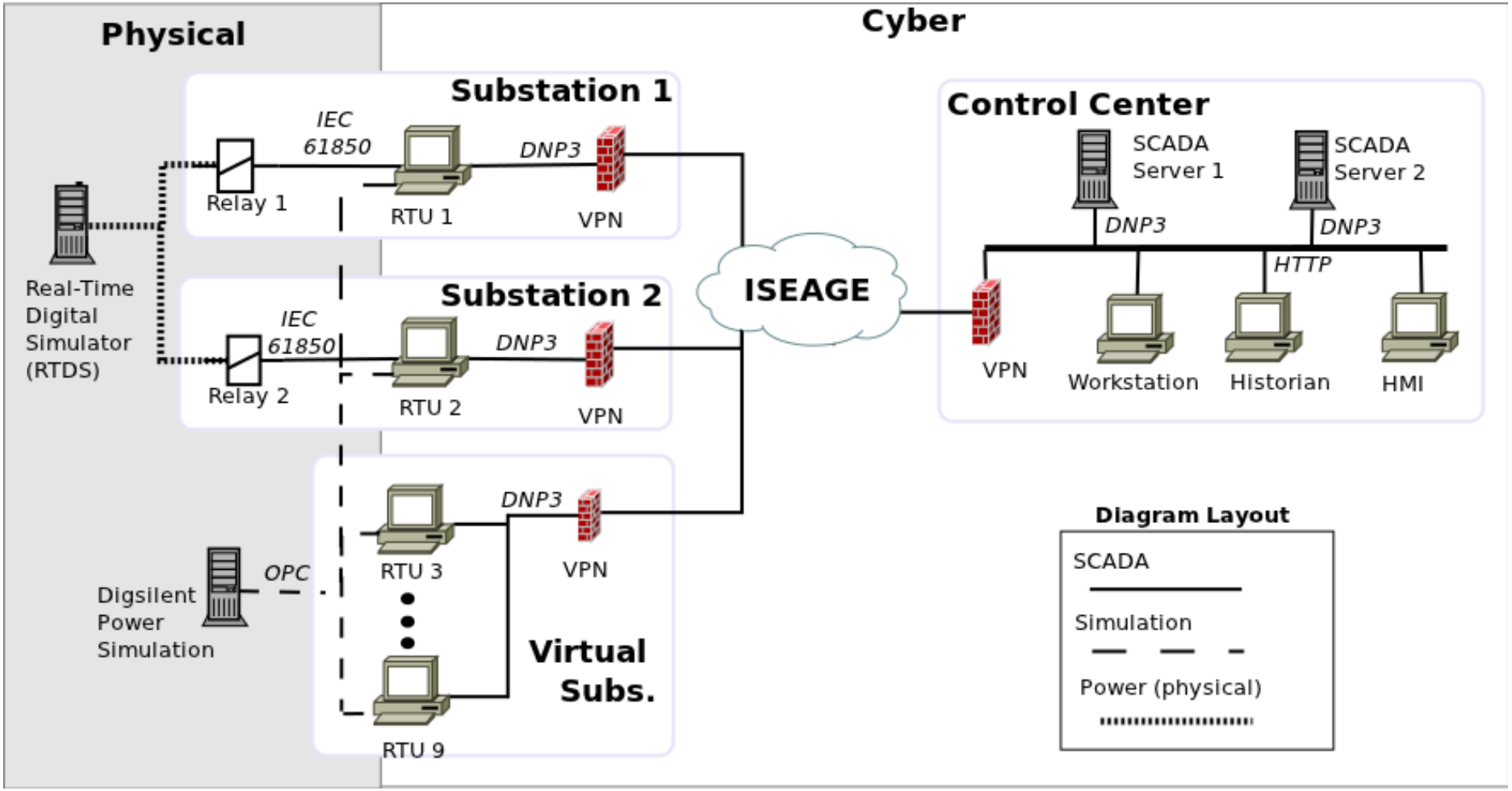


CPS SecurityTestbeds: An Abstraction

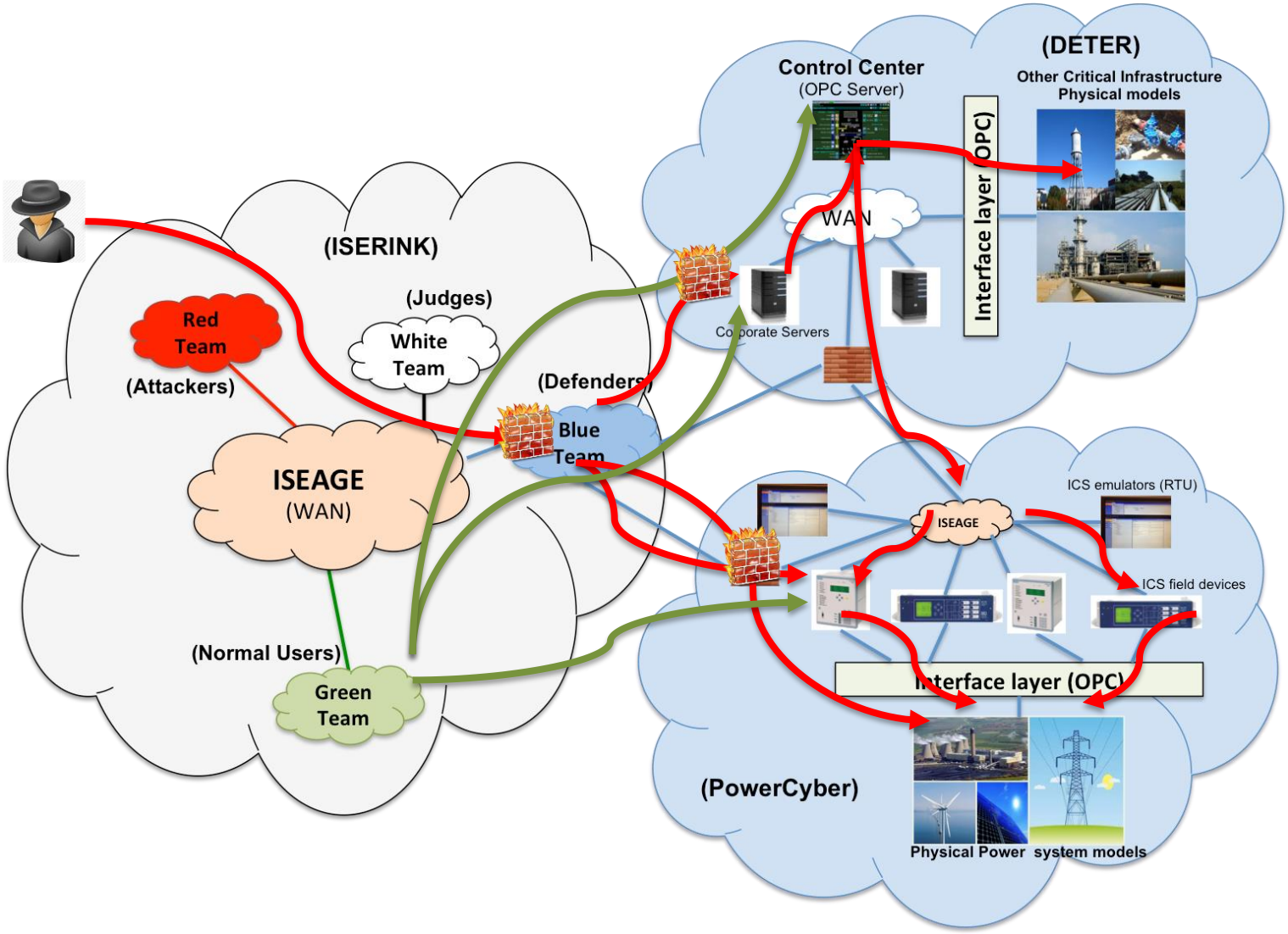


Task 2: ISU *PowerCyber:* CPS Security Testbed

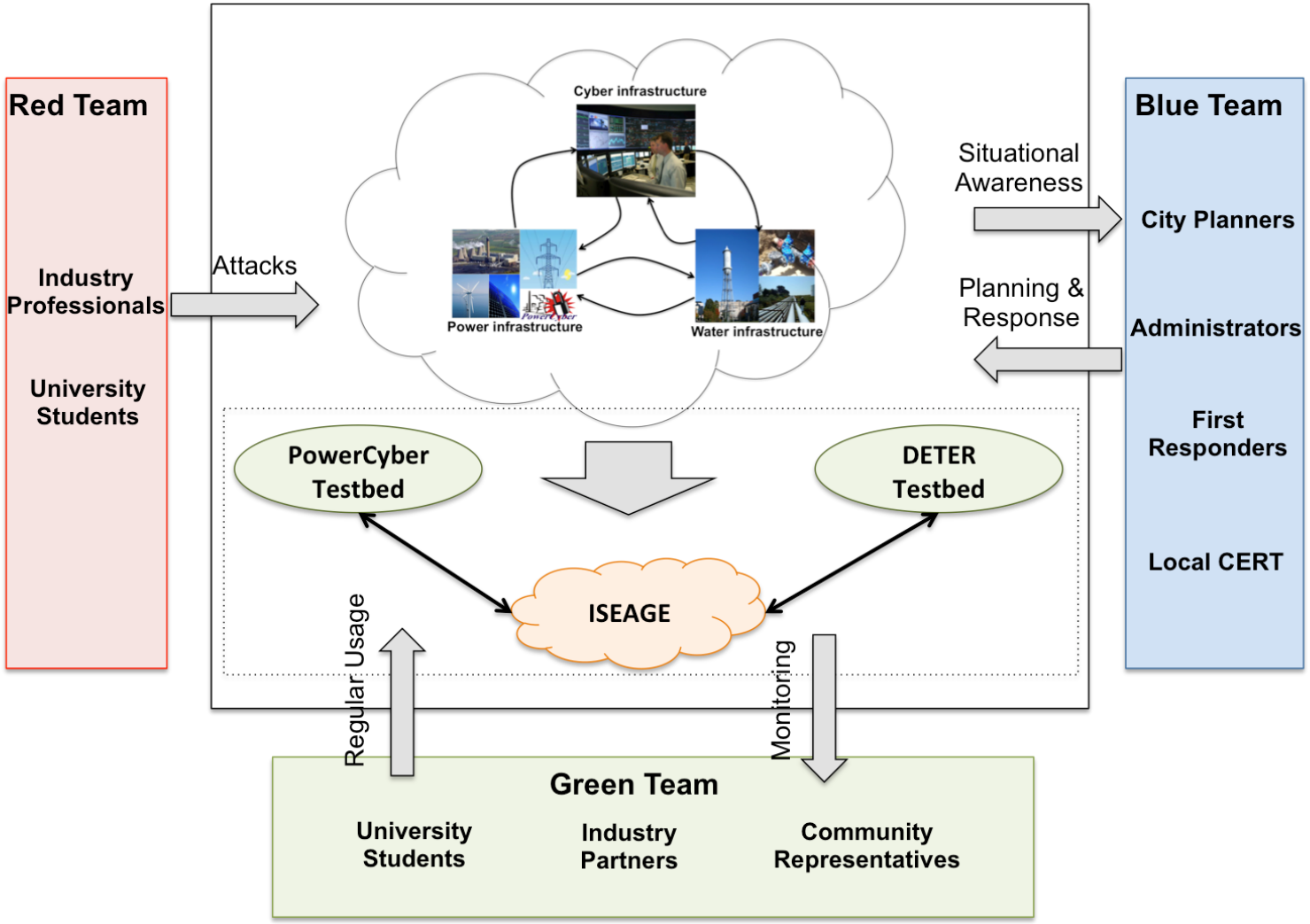
(CPS integration, fidelity, hardware-in-the-loop, cyber-in-the-loop)



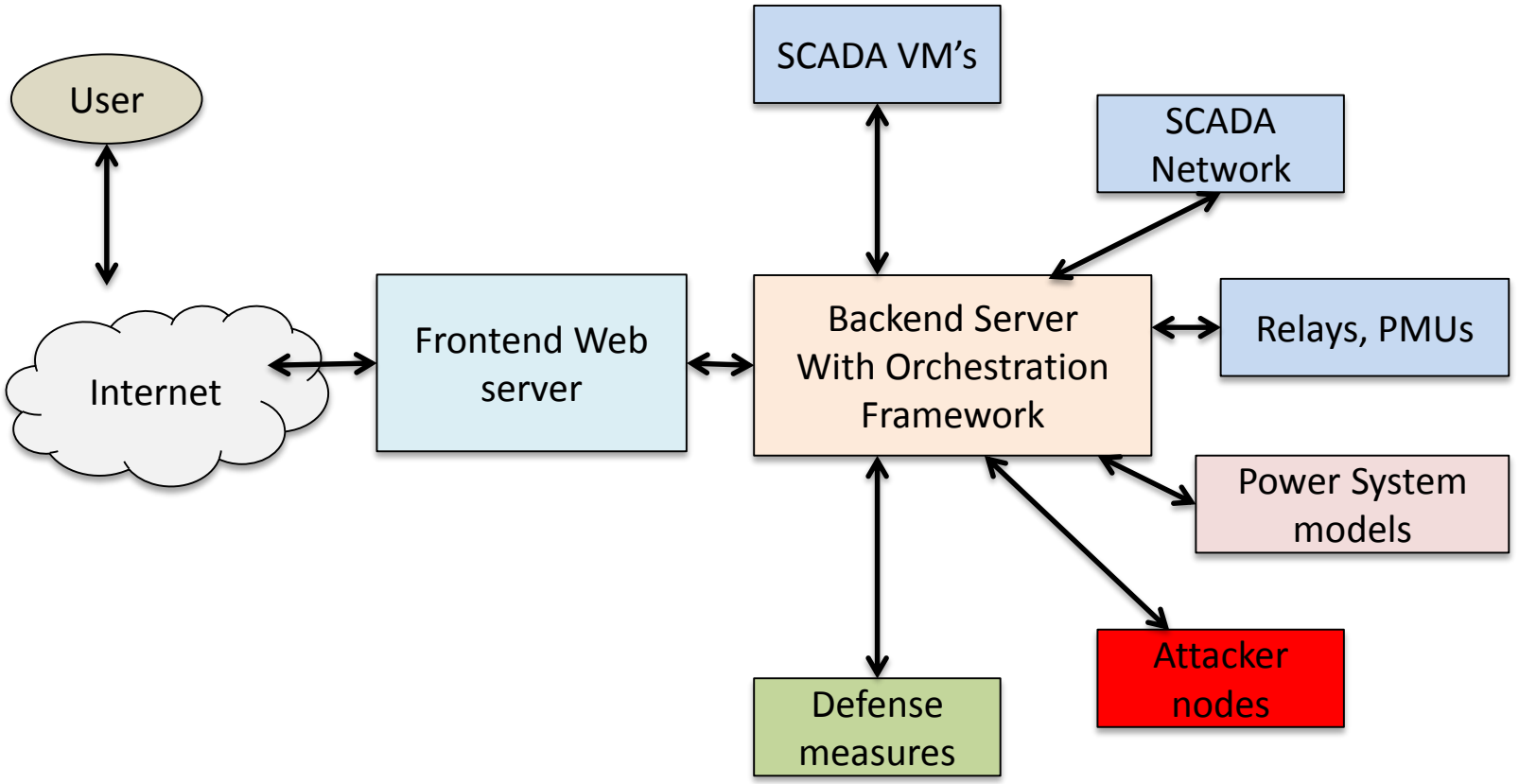
Task 3.1: Testbed Federation & Security Experimentation



Task 3.2: Cyber Defense Competition (CDC)



Task 4: Testbed open interfaces and building Blocks
(front-end, back-end, remote access)



Year 2, Task 1: PowerCyber Testbed Experiments

(Protection and Control Experiments)

CPS Security Testbed – What can it help with?

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.

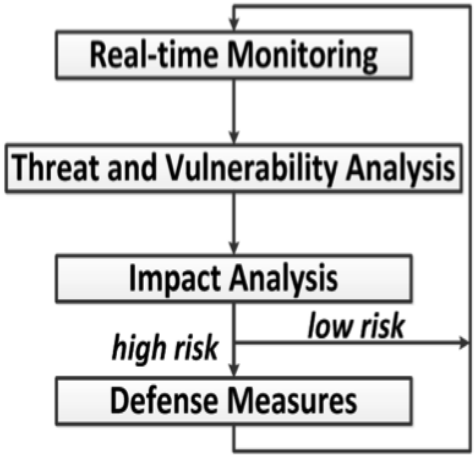
BACKGROUND

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/

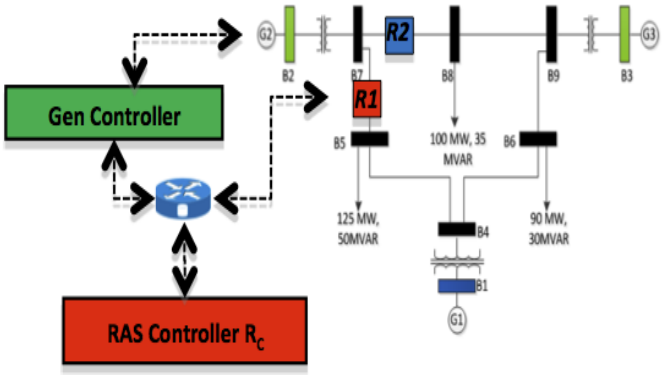
Risk Assessment and Mitigation

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



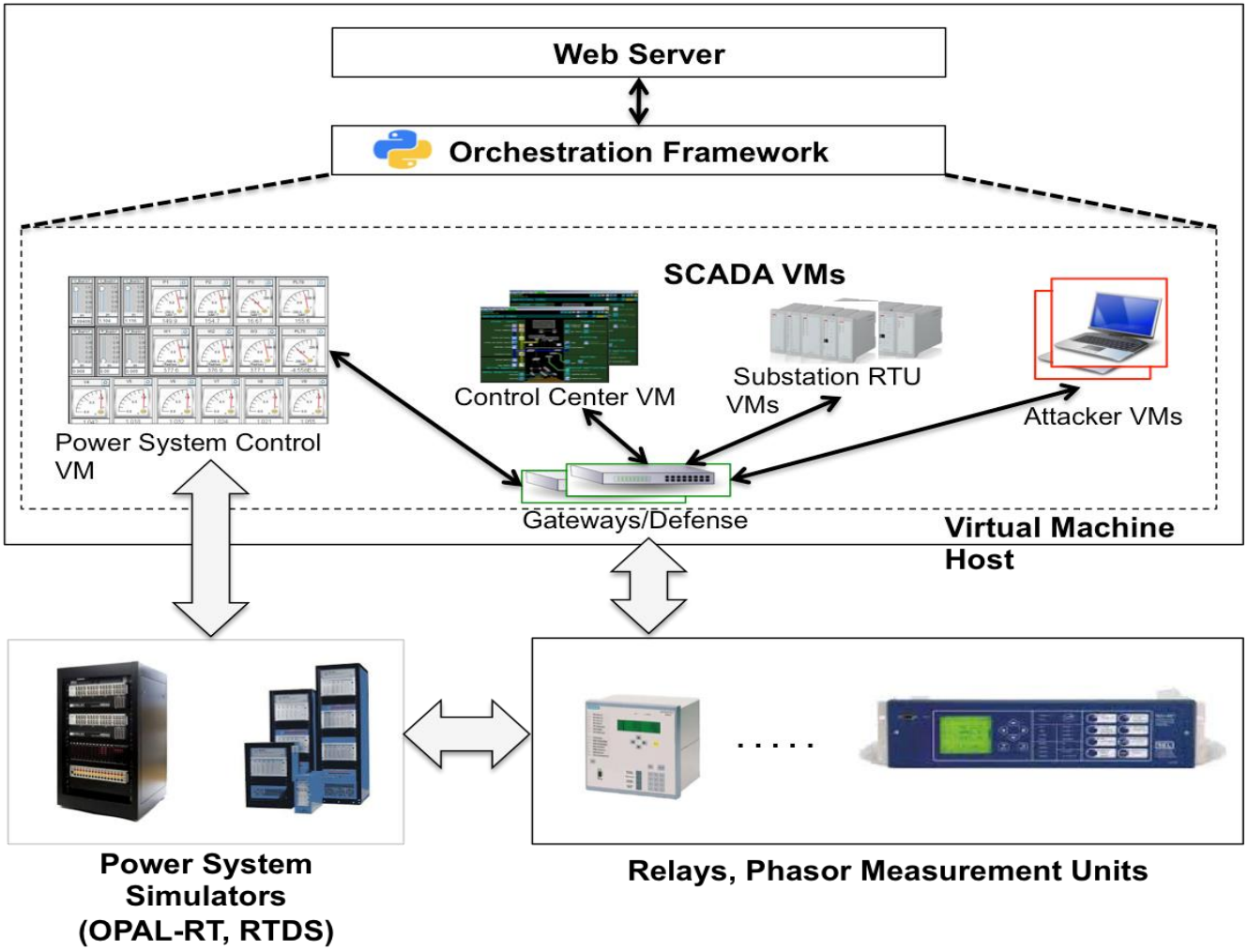
Attack-Defense Evaluations

Attack on Remedial Action Scheme
WECC 9-bus System

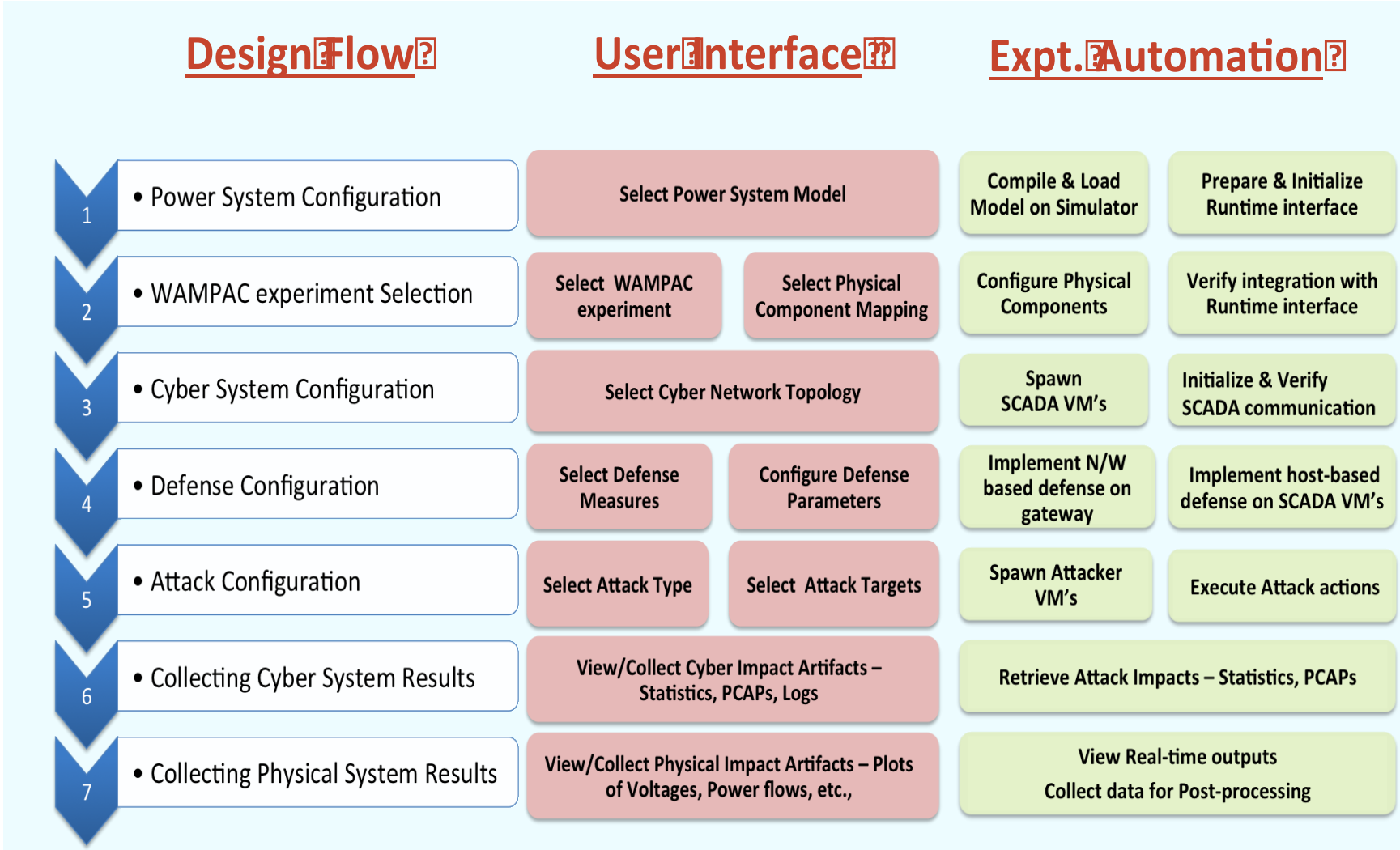


- Data integrity attack to trip R1 + DoS on RAS controller
- R2 trips due to thermal overload; Instability; Load shedding
- Evaluating mitigation schemes

Yr 2, Task 2.1: Expt. Orchestration with Remote Access



Yr 2, Task 2.2: Expt. Orchestration – Design Flow

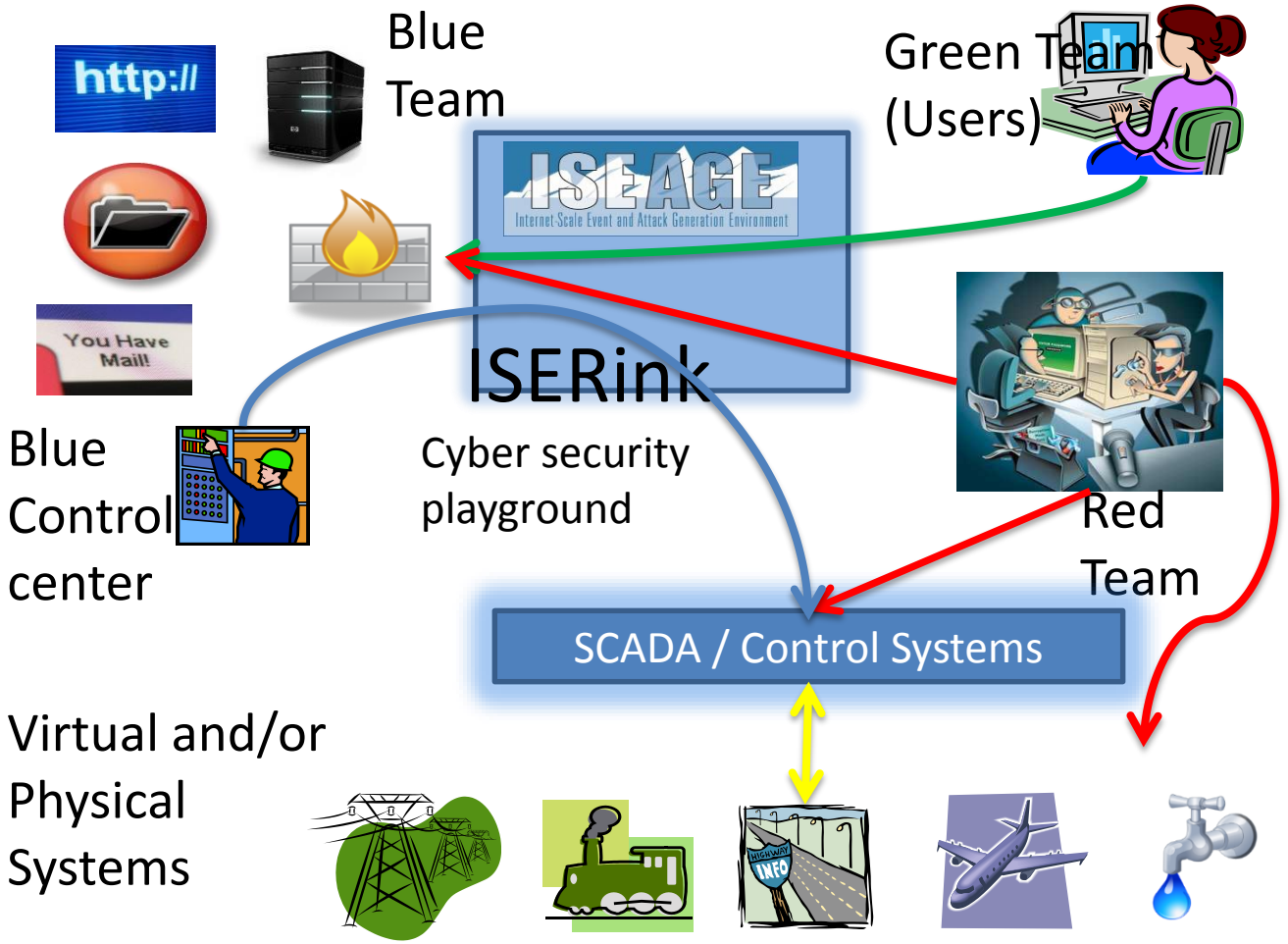


Yr 2, Task 3: Briefing on the Remote Access

- NSF CPS PI meeting Demo, Nov. 16, 2015
- DHS R&D Showcase Demo, Feb. 2016

Yr 2, Task 4.1: Hosting of First CPS-CDC in Feb. 2016

(15 teams, 120 students from multiple universities, industry red team)



Yr 2, Task 5: Early Adopters

Testbed – Research experimentation:

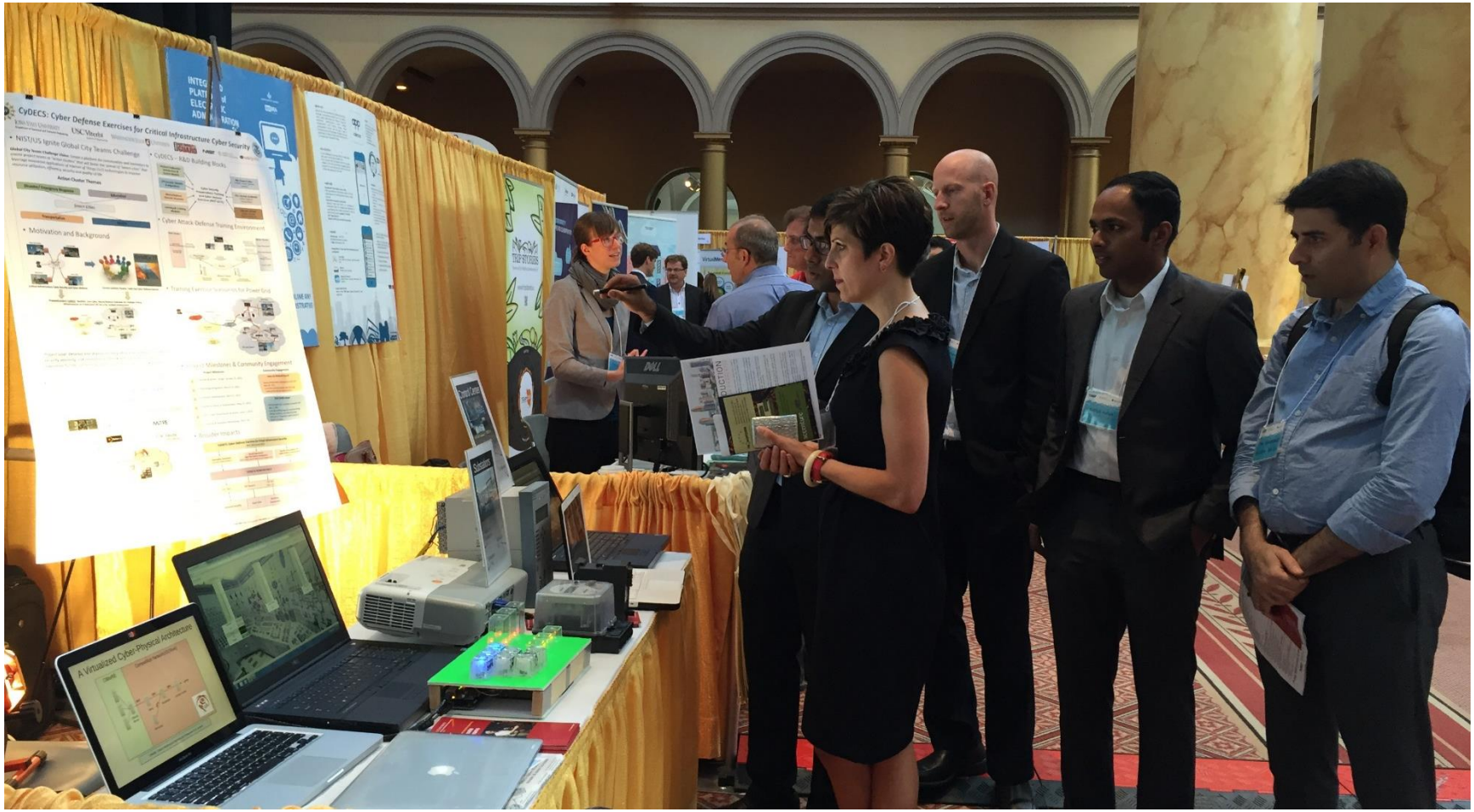
- USC/ISI – DETER project (ongoing)
- Pacific Northwest National Lab (PNNL) - ongoing
- Washington State University (WSU) – being explored

Testbed Early Users:

- Symantec - experimentation (ongoing)
- NERC Industry Training Workshop
- John Hopkins University –ongoing
- University of Minnesota Duluth – planned in March 2016

Yr 2, Task 5.2: Outreach Activities

Demo @ NIST/US-Ignite GCTC Expo 2015



Demo @ NIST/US-Ignite GCTC Expo 2015

Challenges

- Showing early success of remote access
- Developing realistic models and attack vectors
- Sharing of vulnerabilities and results
- Limited programmability, unlike in cyber systems
- Student pipeline

THANK YOU