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

NSF Award # CNS 1446831, Project Managers: David Corman (NSF), Daniel Massey (DHS)

PIs: Manimaran Govindarasu, Venkataramana Ajjarapu, Doug Jacobson
Iowa State University
Graduate Students: Aditya Ashok, Sujatha Krishnaswamy, Matt Brown, Aswin Chidambaram Pappa

Motivation & Project Goals

- Cybersecurity and resiliency of the power grid is of paramount importance to national security and economic well-being.
- CPS security testbeds are enabling technologies that provide realistic experimental platforms for the evaluation and validation of security technologies within controlled environments.

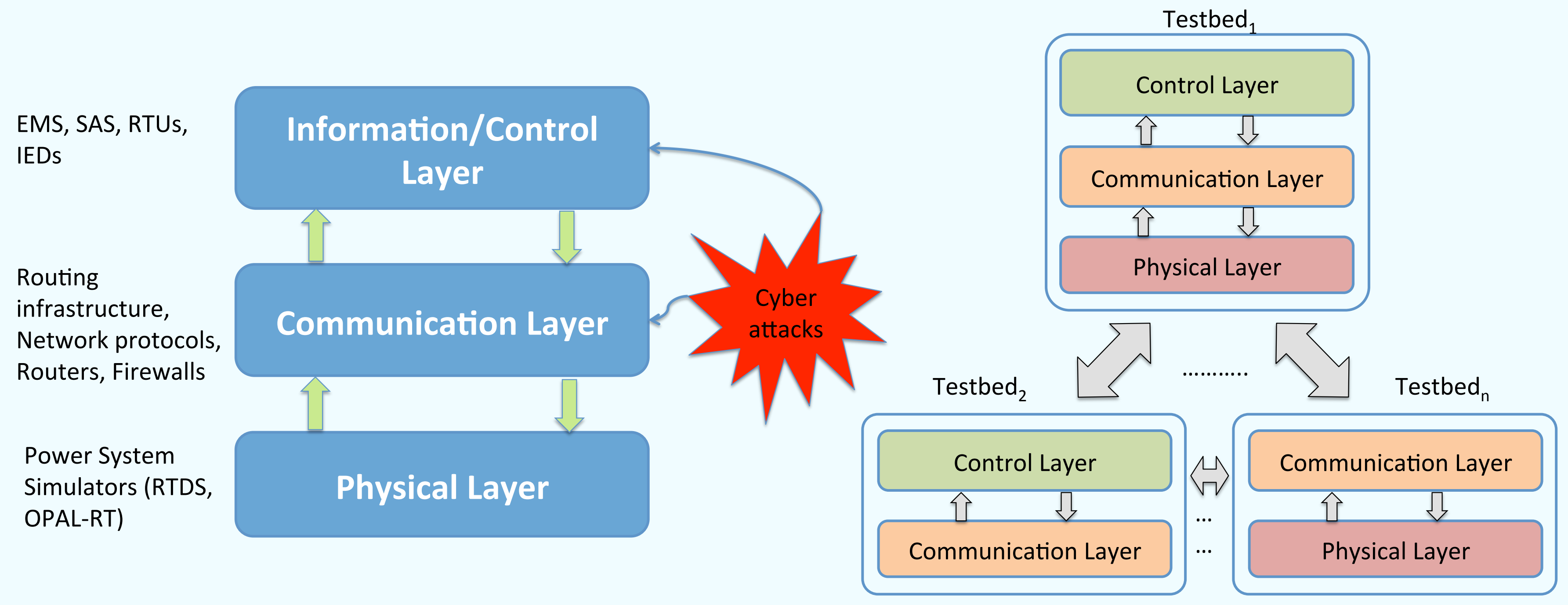
Project Objectives

- Develop innovative architectures, models, and algorithms for large-scale CPS security testbeds.
- Design and implement a high-fidelity, scalable, open-access CPS security testbed for the Smart Grid, and to conduct CPS security research experimentation.
- Develop standardized datasets, models, libraries, and use cases, and make those available to a broader research community through an open, remote-access model by leveraging collaboration from academic and industry partners.
- Develop and disseminate innovative curriculum modules including CPS Cyber Defense Competitions for imparting security knowledge to students via inquiry-based learning.

CPS Security Testbed Federation

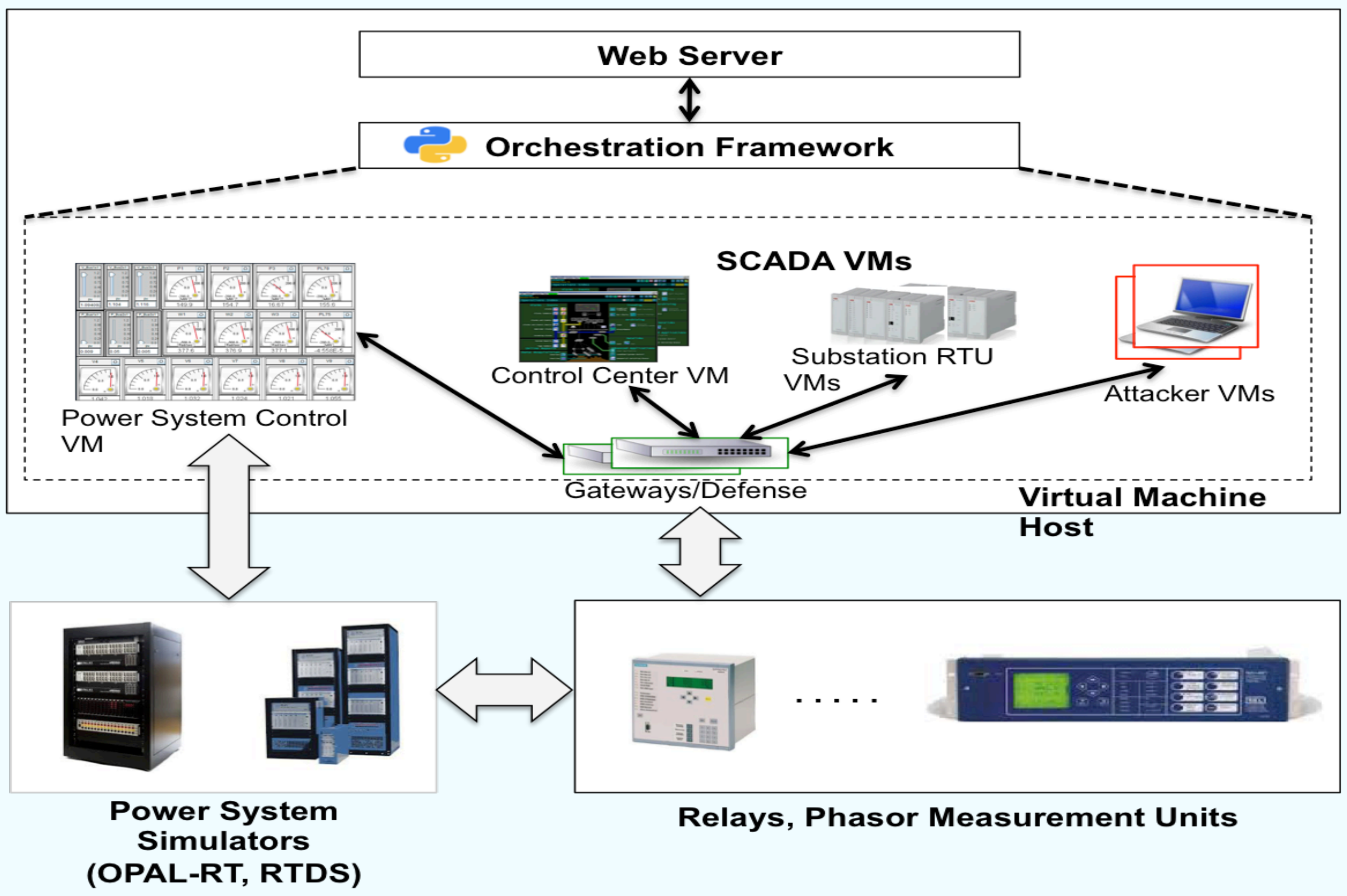
Testbed architecture

Federation architecture



Remote Access CPS Security Testbed

Architecture



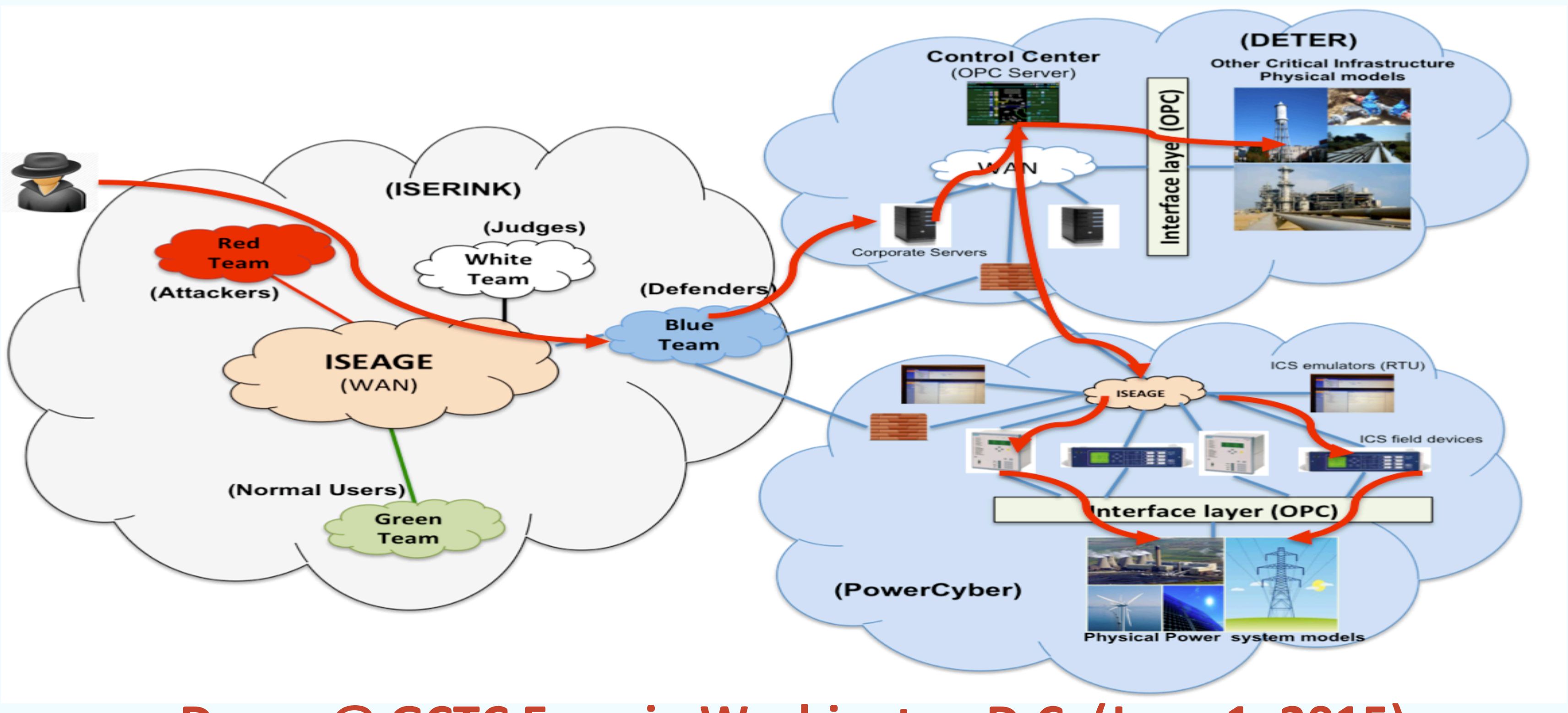
Design Flow	User Interface		Expt. Automation	
1 • Power System Configuration	Select Power System Model		Compile & Load Model on Simulator	Prepare & Initialize Runtime interface
2 • WAMPAC experiment Selection	Select WAMPAC experiment	Select Physical Component Mapping	Configure Physical Components	Verify integration with Runtime interface
3 • Cyber System Configuration	Select Cyber Network Topology		Spawn SCADA VM's	Initialize & Verify SCADA communication
4 • Defense Configuration	Select Defense Measures	Configure Defense Parameters	Implement N/W based defense on gateway	Implement host-based defense on SCADA VM's
5 • Attack Configuration	Select Attack Type	Select Attack Targets	Spawn Attacker VM's	Execute Attack actions
6 • Collecting Cyber System Results	View/Collect Cyber Impact Artifacts – Statistics, PCAPs, Logs		Retrieve Attack Impacts – Statistics, PCAPs	
7 • Collecting Physical System Results	View/Collect Physical Impact Artifacts – Plots of Voltages, Power flows, etc.,		View Real-time outputs Collect data for Post-processing	

NIST/ US Ignite Global City Teams Challenge

Cyber Defense Exercises for Critical Infrastructure 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.*

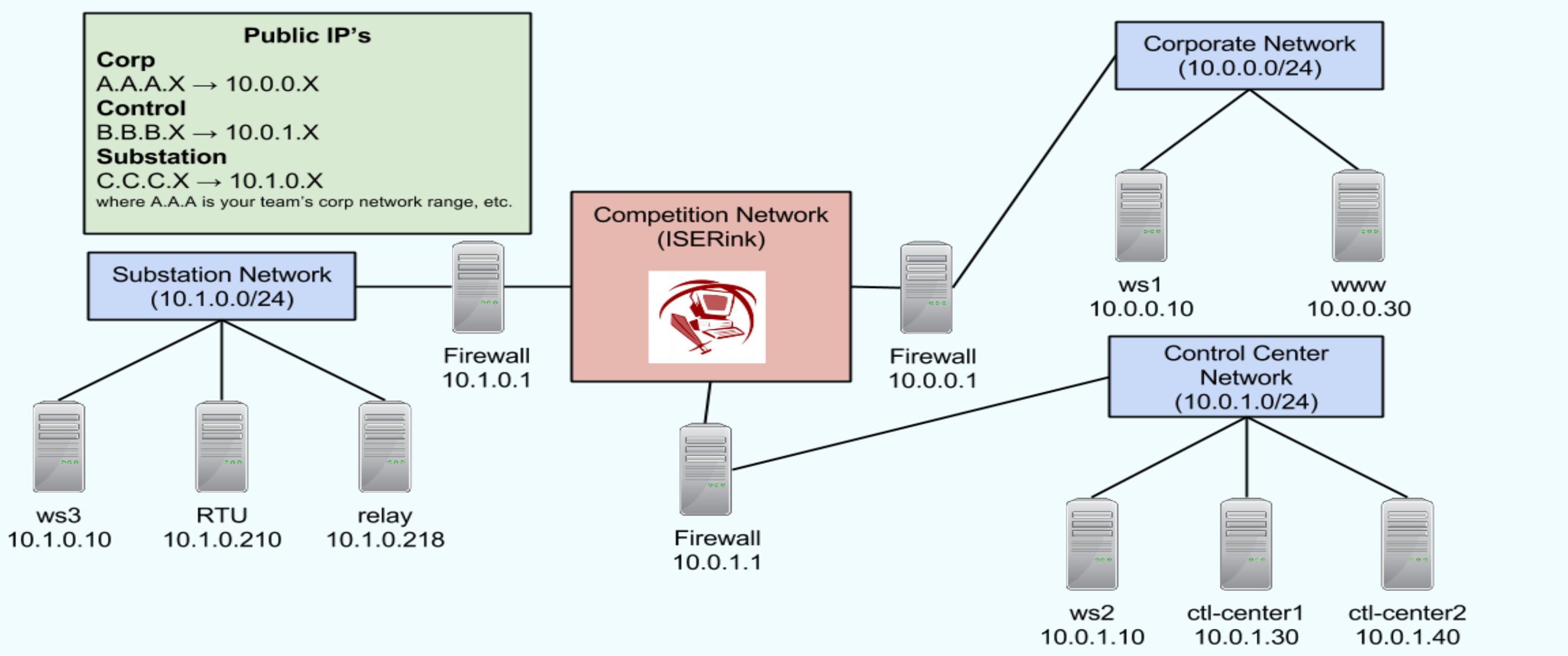
Training Exercise Scenarios on the Federated Testbed



Demo @ GCTC Expo in Washington D.C. (June 1, 2015)

NERC GridSecCon 2015 Training Workshop

Training Environment



Training @ GridSecCon in Philadelphia (October 13, 2015)

User Community Engagement

Use-cases	Institutions
1. CPS Security Research	Pacific Northwest National Lab, Washington State Univ.
2. ICS Cyber Security Research	Symantec Corp., John Hopkins University
3. Education & Training	NERC, Industry Members

Future Work

- **Use-case Scenarios:** Developing a library of models, attack vectors, defenses.
- **Remote Access**: Providing remote access and developing a user community.
- **Testbed Federation:** Develop and implement use-cases for testbed federation.