



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), Christos Papadopoulos (DHS)

PIs: Manimaran Govindarasu, Venkataramana Ajarapu, Doug Jacobson

Postdoc: Gelli Ravikumar; Graduate Students: Vivek Kumar Singh and Burhan Hyder



Motivation & Project Goals

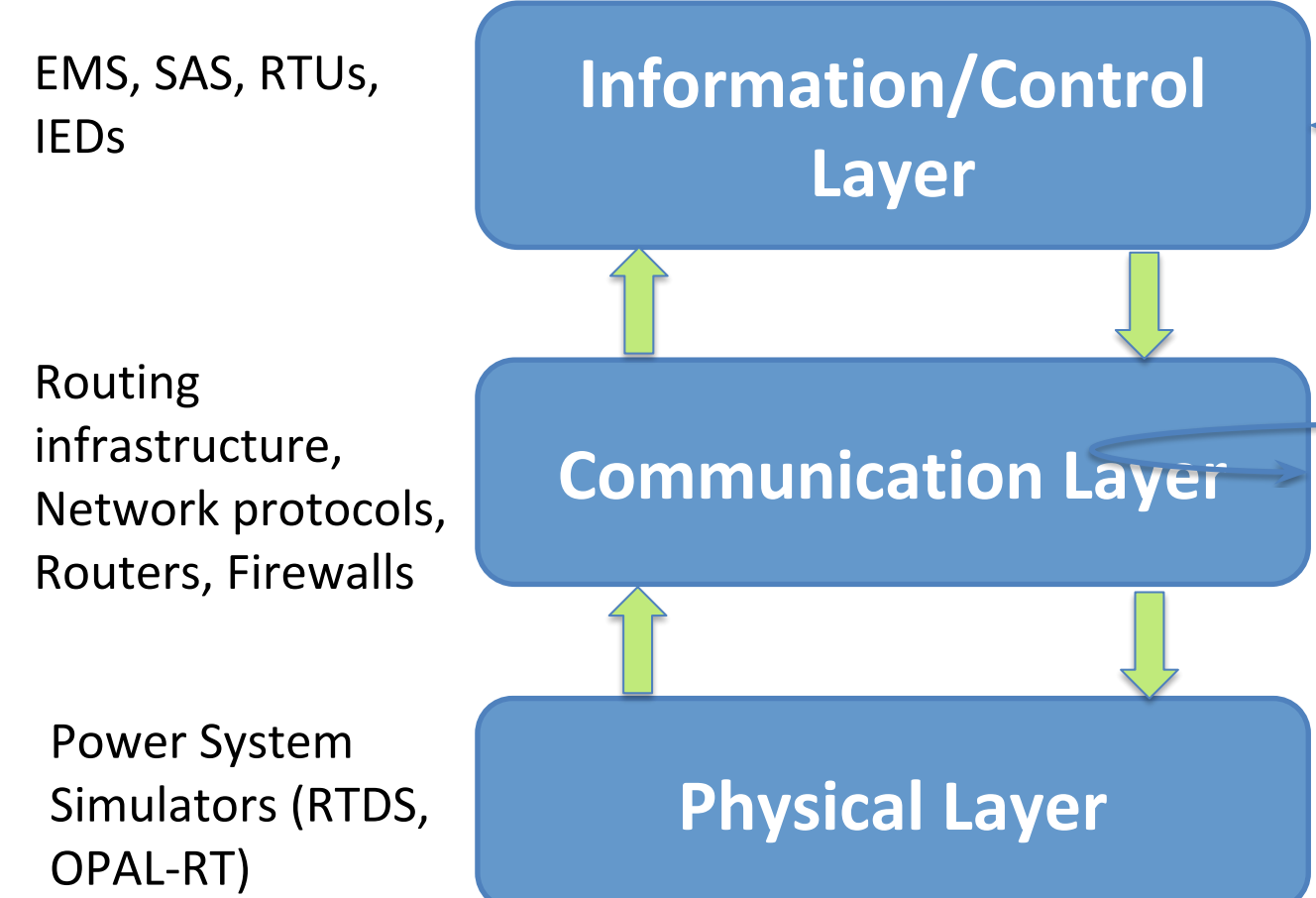
- **Cybersecurity of the power grid** is of paramount importance to national security and economy.
- CPS security testbeds are enabling technologies that provide **realistic experimental platforms** for the evaluation and validation of security technologies within controlled environments.

Project Objectives

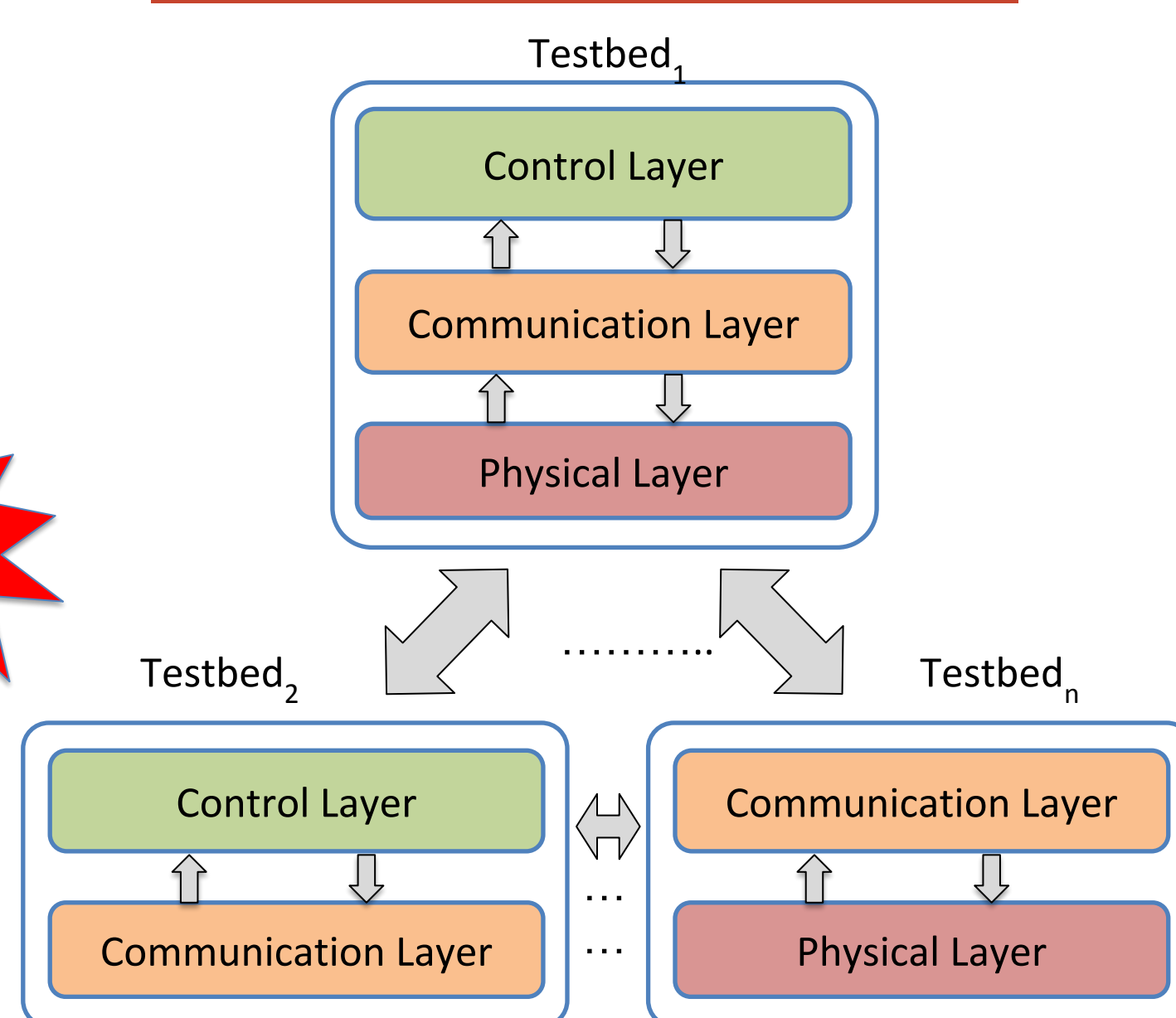
- Develop innovative architectures, models, and algorithms for **large-scale CPS security testbeds**.
- Design and implement a **high-fidelity, scalable, open-access CPS security testbed** for the Smart Grid, and to conduct CPS security research experimentation.
- **Develop standardized datasets, models, 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.

Testbed Architecture and Methodology

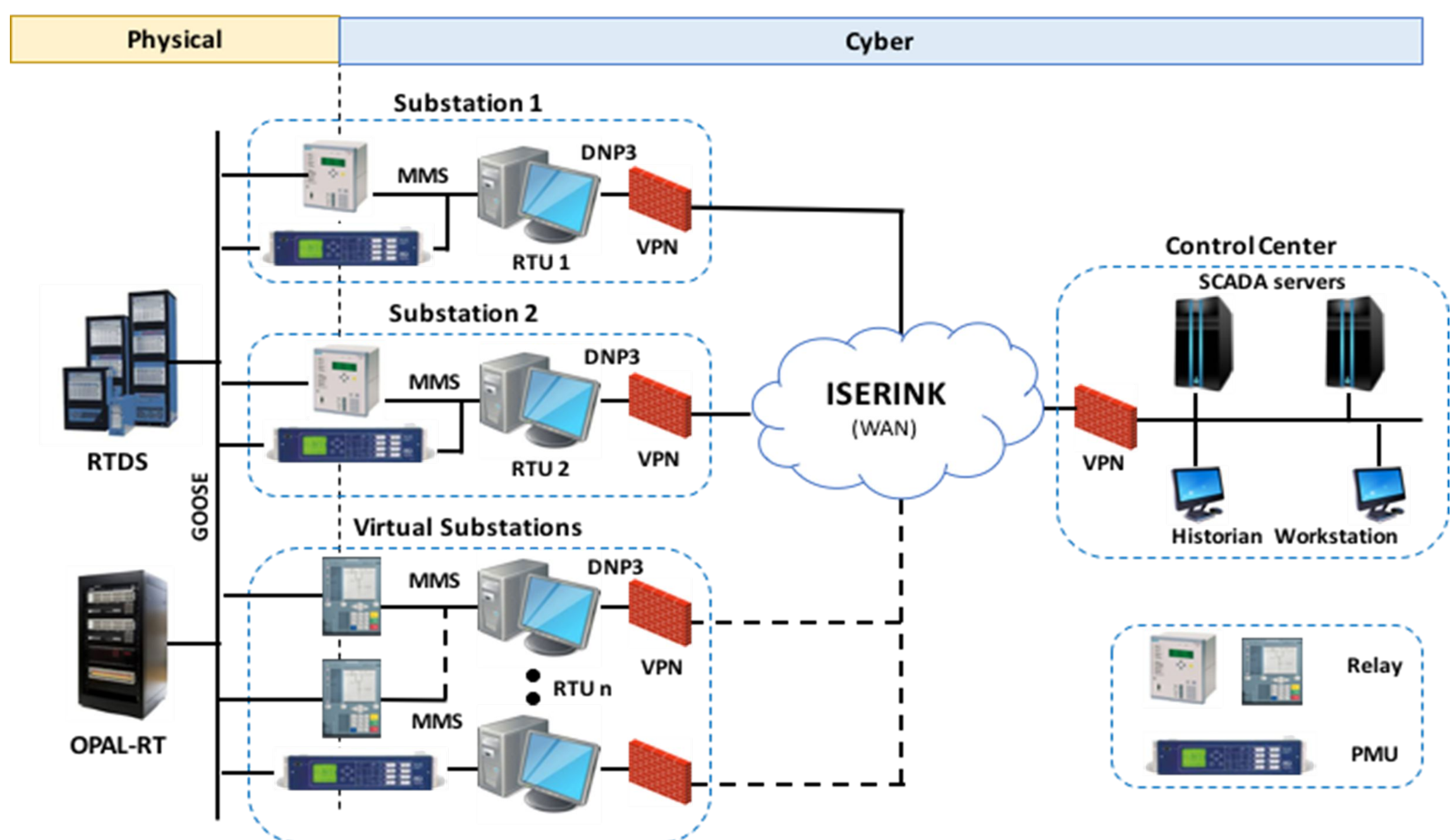
Testbed architecture



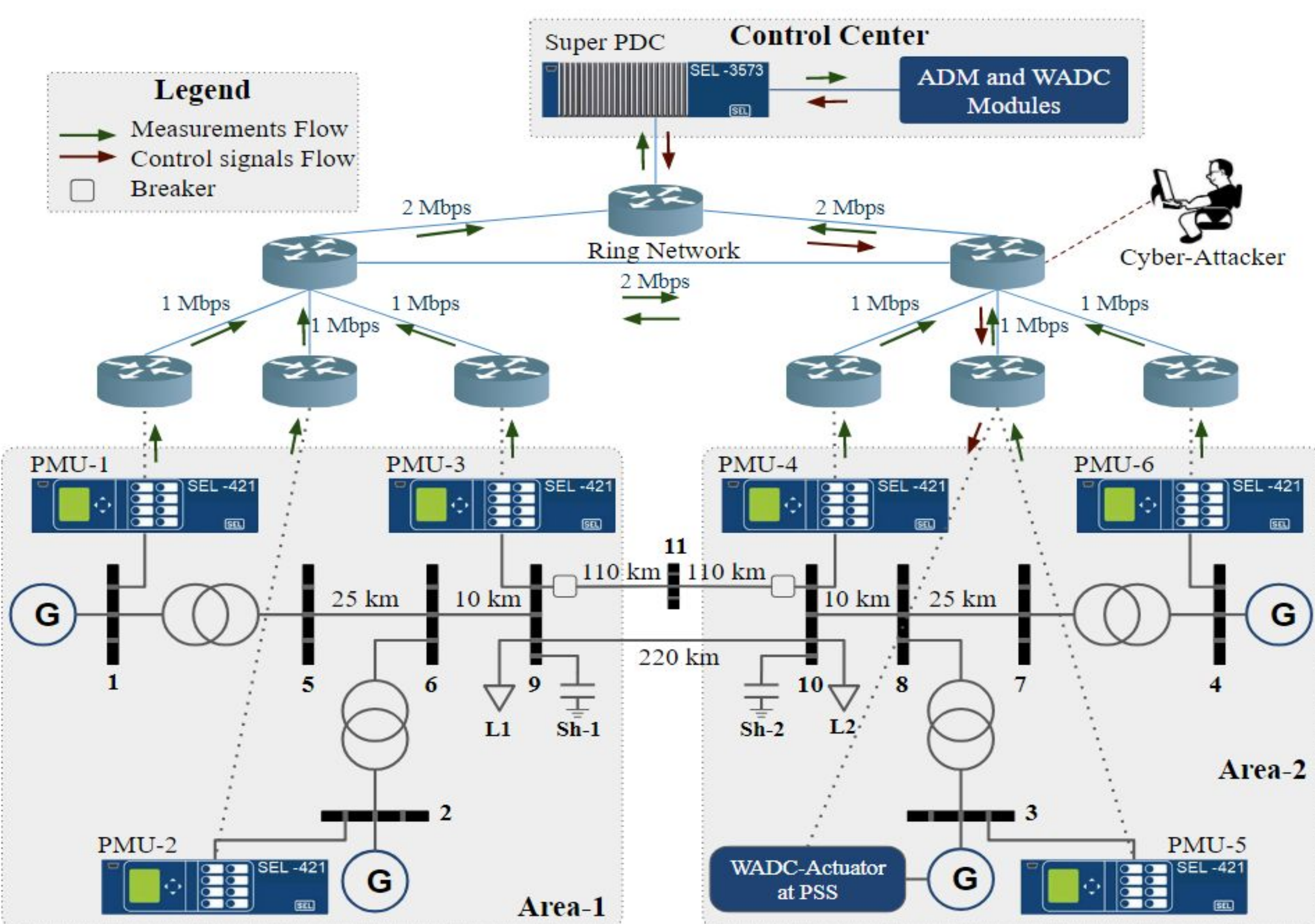
Federation architecture



PowerCyber: Remote Access CPS Security Testbed



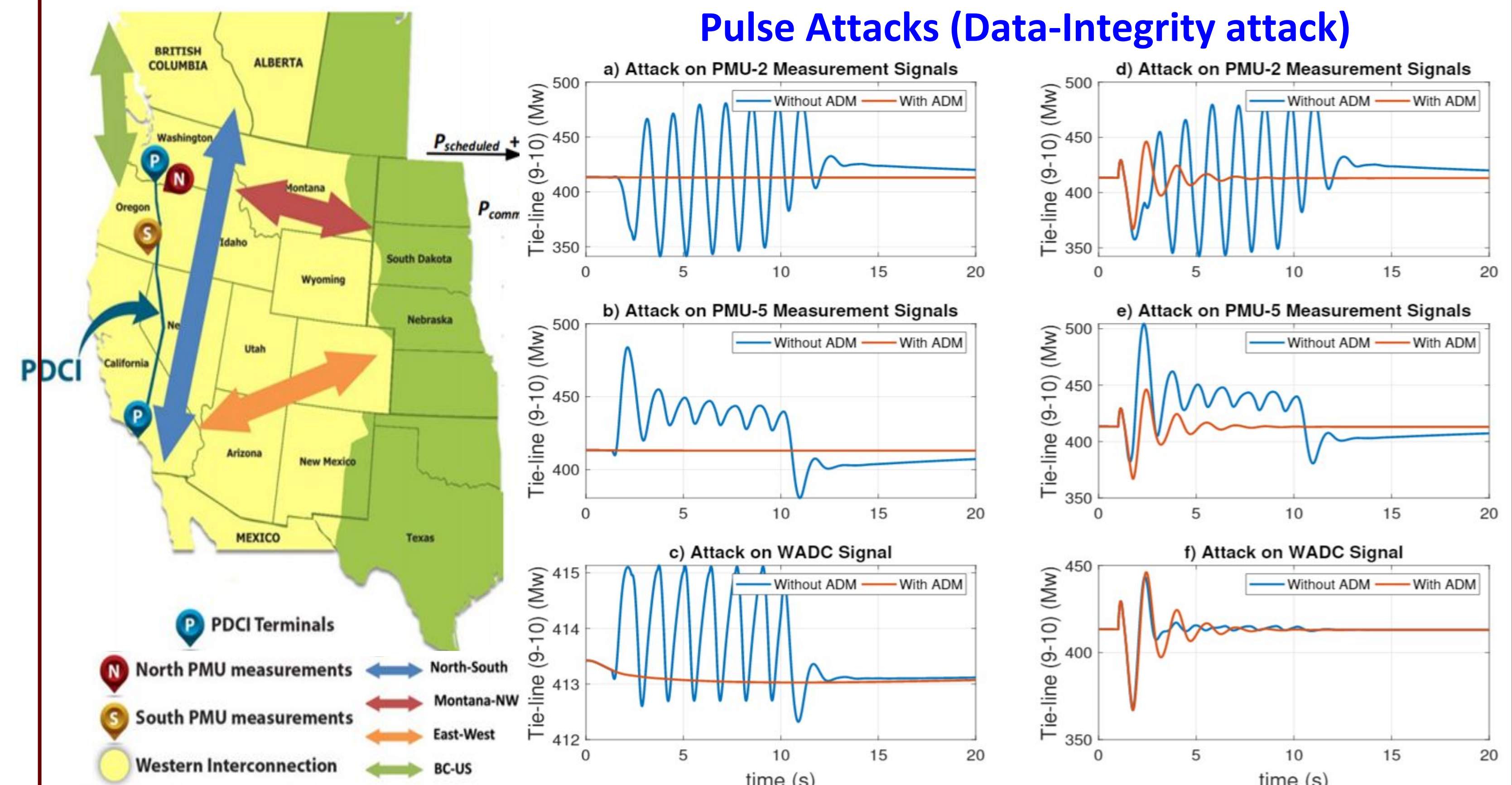
Attack-Resilient Wide-Area Damping Control (WADC) Testbed



R&D Use-cases and Impacts

I. R&D Modeling: Wide-Area Damping Control

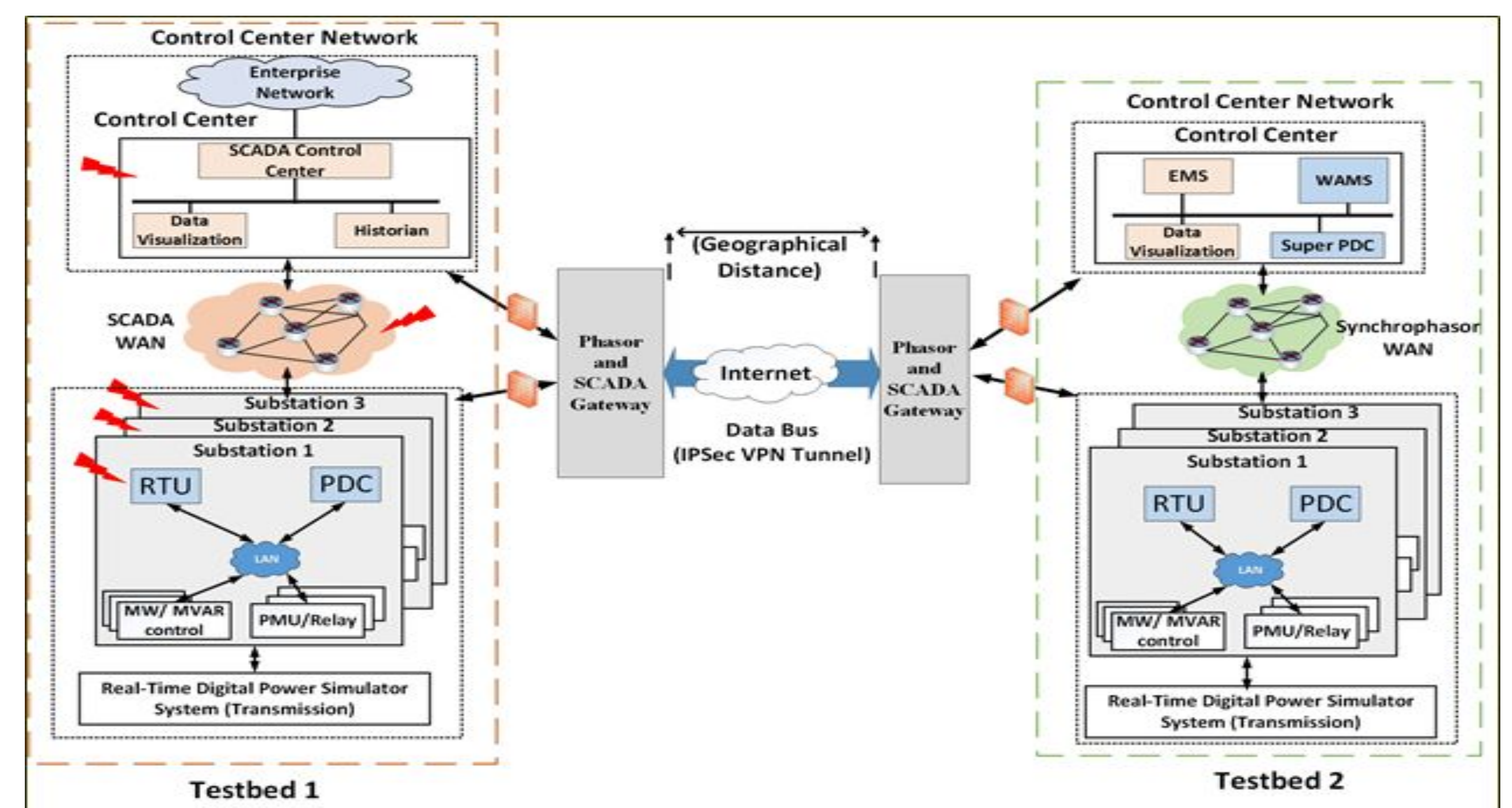
- Proposed **physics-based** and **signal-entropy** based feature extraction to increase the accuracy and robustness of the trained supervisory Machine Learning model.
- Test results witnessed ADM module with **96% accuracy** including low false positive and negative rates for the stealthy data-integrity attacks.



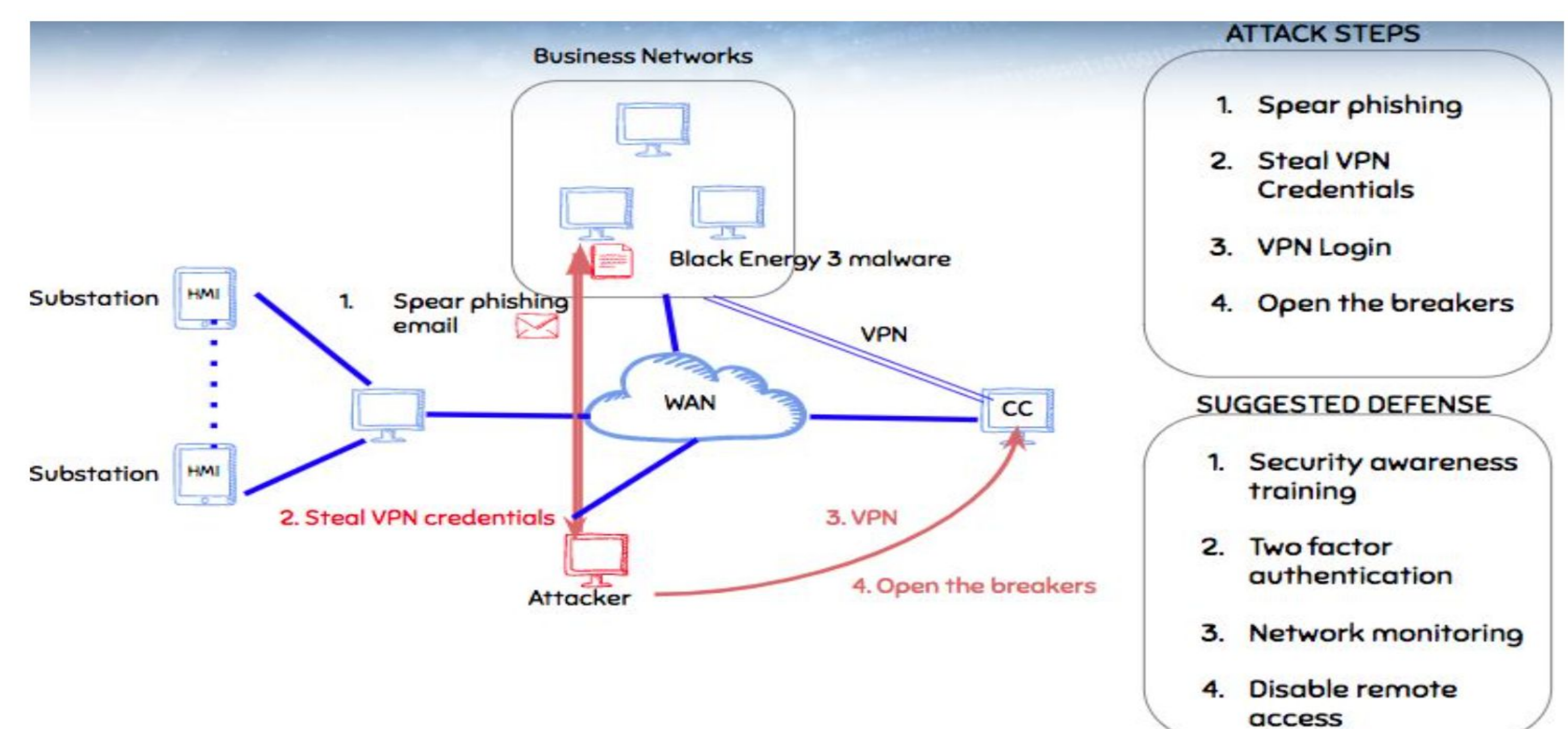
Normal (a-c) and Voltage Perturbation (d-f)

II. Testbed Federation: Wide-Area Monitoring Application

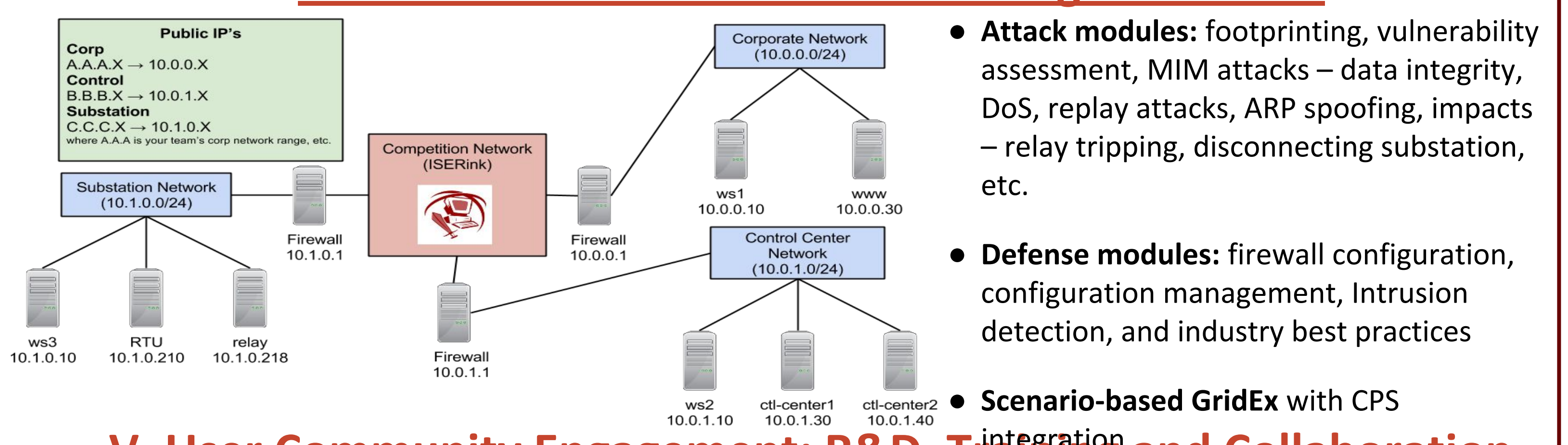
- **Model validation and cyber attack-defense studies** were carried out.
- Measured wide-area latency for synchrophasor data was **26.6 msec**, which is within the industry requirement of 38 msec (by BPA and SCE).



III. Modeling Real Industry Use-case: Ukraine 2015 Attack & Defense



IV. Testbed-based Hands-on Training and GridEx



V. User Community Engagement: R&D, Training and Collaboration

Use Cases	Institutions
Research	PNNL, Symantec, Accenture, John Hopkins University, Army Research Lab
Education and Training	University of Minnesota - Duluth, GridSecCon 2015, 2016 and 2018; Cedar Falls Utilities, MidAmerican, CIPCO, Idaho Power Company, Corn Belt Power Coop, FRCC
International Collaboration	Japan: Tokyo Institute of Technology, CRIEPI (Japan); India: IIT Delhi, IIT Bombay, CPRI; Black Sea Countries: USAID, NARUC