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), Chase Garwood (DHS)

PIs: Manimaran Govindarasu, Venkataramana Ajjarapu, Doug Jacobson

Iowa State University

Graduate Students: Pengyuan Wang, Subramanian Arunachalam, and Vivek Singh

Motivation & Project Goals

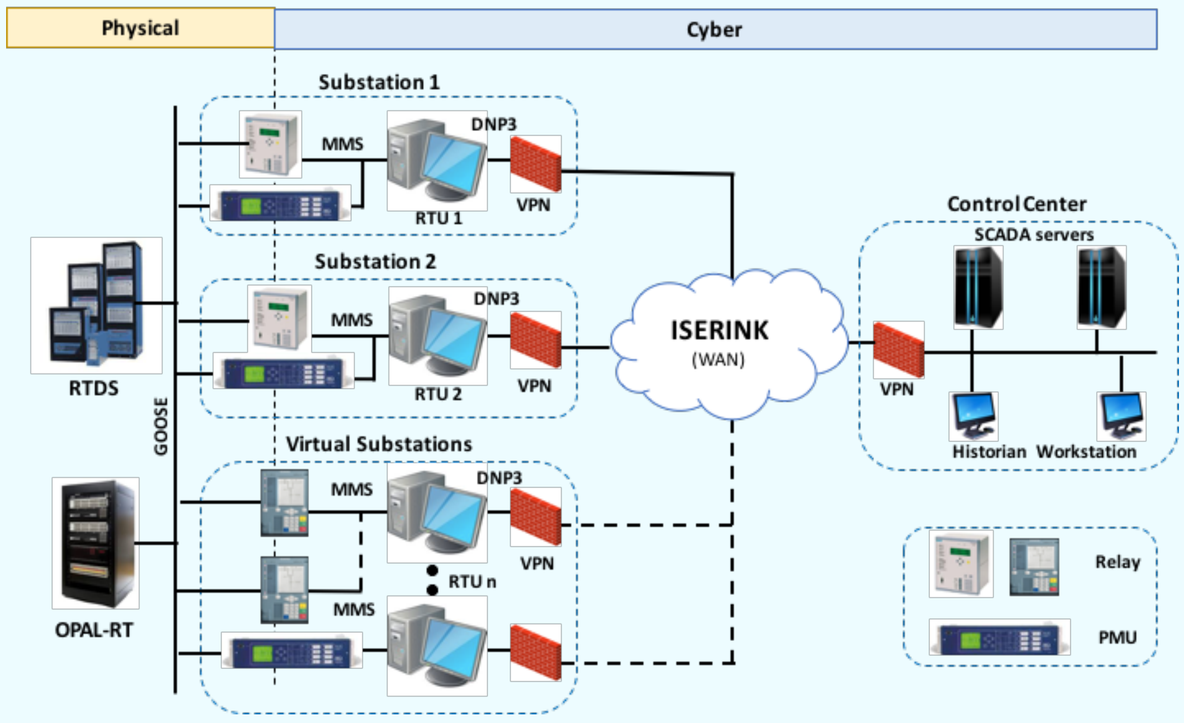
- Cybersecurity and resiliency of the power grid is of paramount importance to national security and economic well-being.
- CPS security testbeds are enabling technologies that provide realistic experimental platforms for the evaluation and validation of security technologies within controlled environments.

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.

Remote Access CPS Security Testbed

Architecture

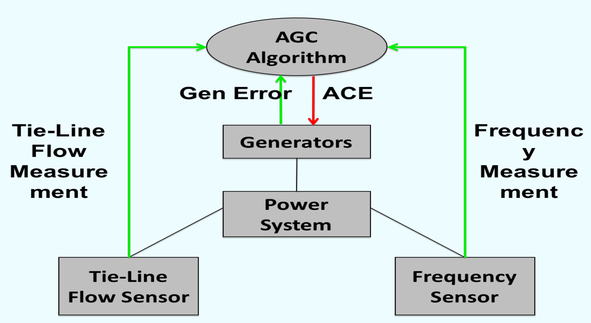


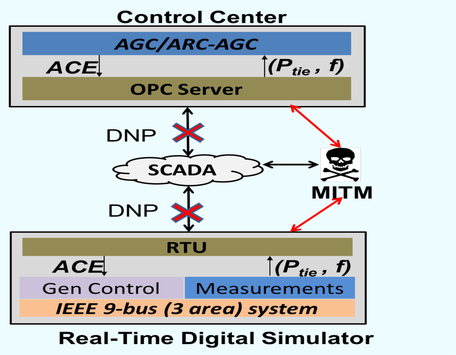
Design Flow

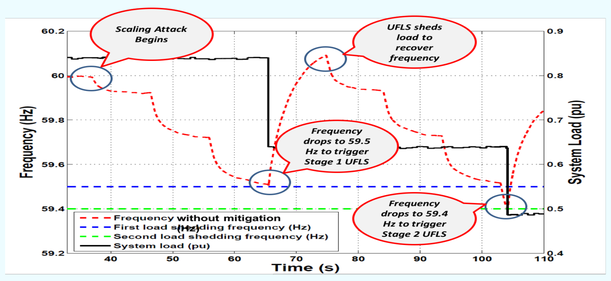
1	• Power System Configuration	Select Power System Model	Compile & Load Model on Simulator	Prepare & Initialize Runtime interface
2	• WAMPAC experiment Selection	Select WAMPAC experiment / Select Physical Component Mapping	Configure Physical Components	Verify integration with Runtime interface
3	• Cyber 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	

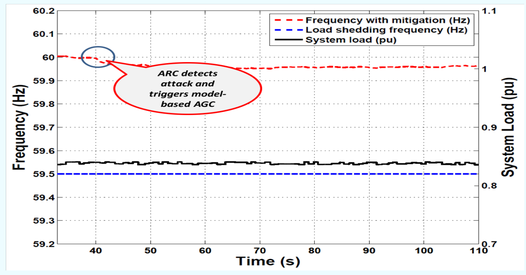
Remote Access Story Boards

MITM attack Impact and Attack Resilient AGC Control

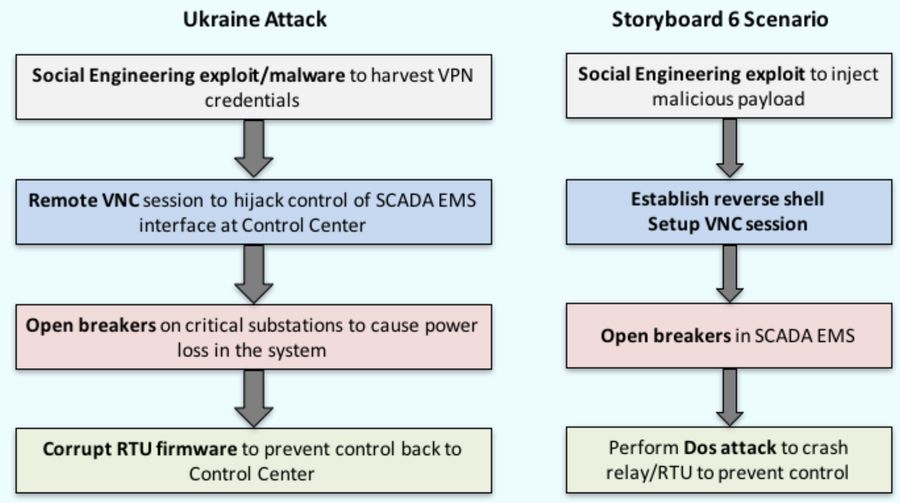








Mapping Realistic Scenarios to Storyboards



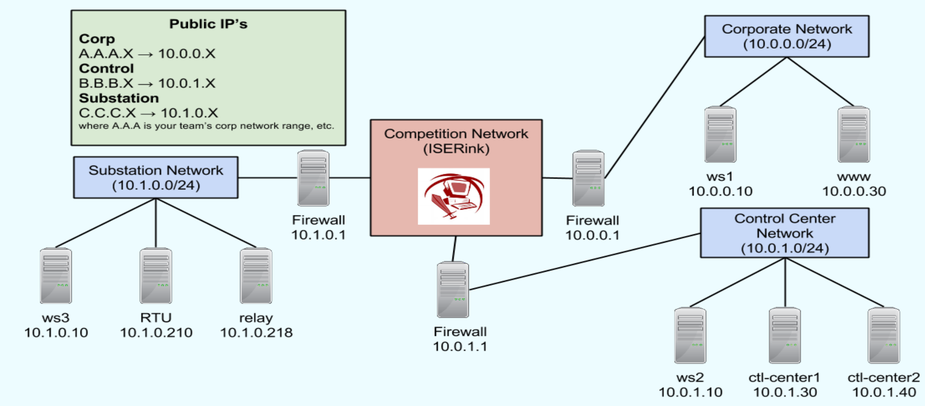
Attack & Defense Measures for Storyboards

#	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

#	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	

Cybersecurity Training for Industry

Remote Access Testbed Training Environment



User Community Engagement

Use-cases	Institutions
1. CPS Security Research	Pacific Northwest National Lab, Washington State Univ.
2. ICS Cyber Security Research	Symantec Corp., Accenture Labs, John Hopkins University
3. Education & Training	University of Minnesota, Duluth, NERC, EPRC members
4. International study tour	Tokyo Institute of Technology, Black sea area utilities

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.

IOWA STATE UNIVERSITY
Department of Electrical and Computer Engineering

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