PowerCyber: Cyber-Physical Security Testbed Training for Smart Grid

PI: Manimaran Govindarasu (gmani@iastate.edu)

Postdoc: Gelli Ravikumar (gelli@iastate.edu)

Graduate Students: Vivek Kumar Singh, Burhan Hyder, Sathya Mohan, Srayashi Konar, Pengyuan Wang, Jacob Drahos, and Jacob Ulrich

Department of Electrical and Computer Engineering, Iowa State University, Ames, Iowa, USA.

IOWA STATE UNIVERSITY

powercyber.ece.iastate.edu

Cybersecurity for Smart Grid

Objective

The goal of the CPS security training is to provide practical scenario-based hands-on learning experience for the participants in cyber attack-defense methodology for smart grid using industry-grade SCADA platform and state-of-the-art security practices and tools.

Learning Outcomes

Outcomes

- Ability to identify and analyze attack vectors to the grid environment
- Ability to use modern cybersecurity tools for attack-defense such as network reconnaissance, vulnerability assessment, firewall configuration, intrusion detection/prevention.
- Ability to perform scenario-based Risk analysis
- Ability to perform impact characterization for cyber-attack scenarios

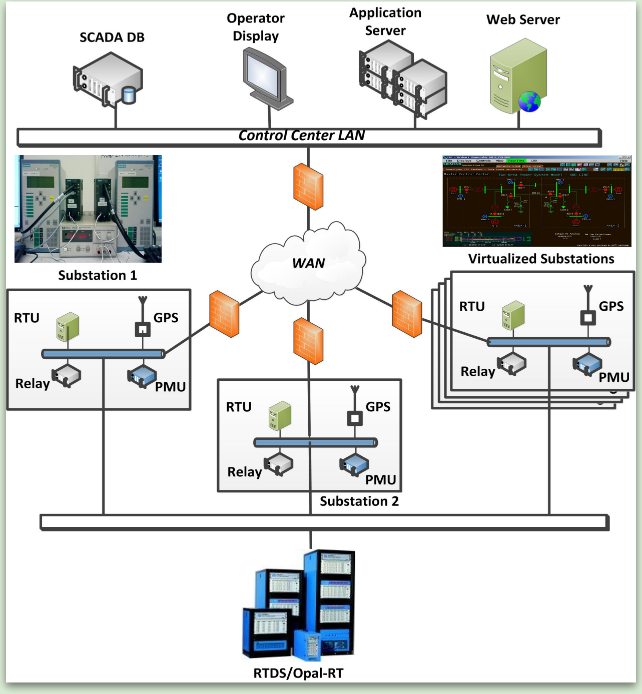
CPS Testbed-based Cybersecurity Training Platform

Usecases

- Cyber Attack-Defense Evaluation
- Vulnerability Assessment
- Systems Impact Analysis
- Security Product Testing
- Risk Assessment
- Risk Mitigation Studies
- Education
- Industry Short-Courses

Salient Features

1. **Hardware-in-the-Loop Real-Time Testbed for modeling smart grid**
   a. Industry-grade SCADA/EMS and Substation platform
   b. GNS3-based and ISEAGE-based WAN emulation; DNP3 and IEC-61850 SCADA protocols; Industry-grade cybersecurity software systems.
   c. Wide-area control and protection applications interfaced with Hardware-in-the-Loop (HIL) CPS Testbed including Opal-RT/RTDS.
2. **Scalability, Modularity and High Fidelity:**
   a. RTDS/Opal-RT provide ability to simulate large power systems with control and protection functions in real-time.
   b. Multi-area substation architecture enabled through virtualization.
   c. Testbed-based federation for smart grid applications.
3. **Remote Access:** Web-based access for remote experimentation with custom power/cyber system models and attack templates.



Basic CPS Security Training

Training Modules	Applicable NERC CIP Standards
Module 0: Introduction	CIP – 004: Personnel and Training
Module 1: Network Scanning	CIP – 0010: Configuration Change Management and Vulnerability Assessments
Module 2: Vulnerability Assessment	
Module 3: Attack Exercise – Relay tripping	CIP – 0010: Configuration Change Management and Vulnerability Assessments CIP – 0011: Information Protection CIP – 0012: Physical Security
Module 4: Defense: Firewall configuration	CIP – 003: Security Management Controls CIP – 005: Electronic Security Perimeter(s) CIP – 007: Systems Security Management CIP – 010: Configuration Change Management and Vulnerability Assessments
Module 5: AttackSurface Host Analyzer (AHA)	
Module 6: SIEM and IDS	
Module 7: Attack-Defense case studies	

Advanced CPS Security Training

Hardware-in-the-Loop CPS Training (WAMPAC and SCADA)
Module 11: Wide-Area Monitoring
Module 12: Wide-Area Damping Control
Module 13: Wide-Area Voltage Control
Module 14: Wide-Area Protection - Remedial Action Schemes
Module 15: Automatic Generation Control
Module 16: Distributed SIEM IDS for the Multiple Substations
Module 17: Scenario-based Attack-Defense: Ukrainian Power Grid 2015

Trainings Chronology	**Year**	2015/2016	2017	2018
	Industry Users	GridSecCon 2015, GridSecCon 2016, EPRC	MidAmerican Energy Company, CIPCO, Cedar Falls Utilities	Alliant Energy, GridSecCon 2018, Idaho Power Company, Corn Belt Power Cooperative, MISO