PowerCyber: A Cyber-Physical Security Testbed for Smart Grid

PI: Manimaran Govindarasu (gmani@iastate.edu)

Collaborators: Venkataramana Ajjarapu, Doug Jacobson, Umesh Vaidya

Department of Electrical and Computer Engineering

Iowa State University, Ames, IA 50011

powercyber.ece.iastate.edu

NSF Grants: CNS-0915945, ECCS 1202542

Cyber Security for Power Systems – Why?

Abstract - Electric power grid is a complex cyber physical system (CPS) that forms the lifeline of modern society, and its reliable and secure operation is of paramount importance to national security and economic vitality. Cyber security of the power grid — encompassing attack prevention, detection, mitigation, resilience, and deterrence — is among the most important R&D priorities today. Iowa State's ***PowerCyber*** testbed provides a unique cyber-physical integration for bulk power system wherein, **vulnerability analysis, system impact studies, risk assessment,** and **attack-defense evaluations** are being carried out. Also, it has potential to offer high-fidelity, highly-scalable, remotely accessible, and federated environment for cyber security experimentations.

CPS Security Testbed – What do we have?

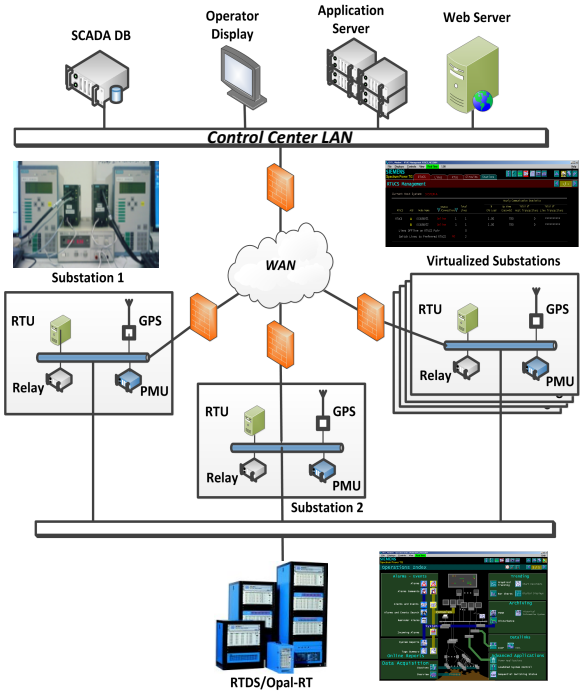
Capabilities

- Vulnerability Assessment
- System Impact Analysis
- Risk Assessment
- Risk Mitigation Studies
- Attack-Defense Evaluations
- Security Product Testing
- Education & Industry Short Course
- Guidance for NERC CIP compliance

Salient Features

1. ***Cyber-in-the-Loop Real-Time Simulation*** environment modeling bulk power system for cyber security experimentations.
2. ***Scalability:***
   - Real-Time simulators, RTDS/Opal-RT, provide ability to simulate large power systems with monitoring, protection, control functions.
   - Multi-area, substation architecture enabled through virtualization.
3. ***High Fidelity:***
   - Industry-grade SCADA/EMS and substation automation.
   - WAN emulation using ISEAGE; DNP3 and IEC61850 protocols used for SCADA; Industry-grade security appliances for VPN/firewall.
   - Local/wide-area control and protection applications emulated with programmable IEDs and PMUs interfaced with RTDS/Opal-RT.
4. ***Remote Access***: Web-based access for remote experimentation with custom power/cyber system models and attack templates.

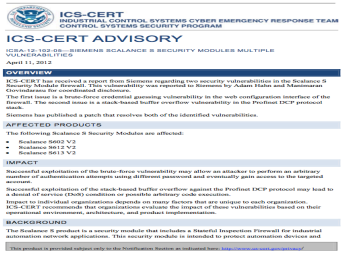
Architecture



CPS Security – What can we do?

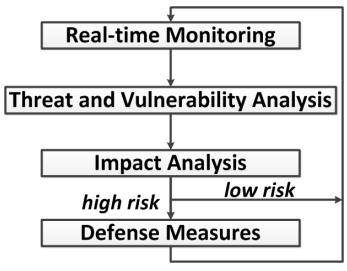
Vulnerability Assessment

- Vulnerability assessment of field devices (relays, IEDs, PMUs), protocols, automation software
- Penetration testing
- Responsible vulnerability disclosure



Risk Assessment and Mitigation

- Risk = Threat * Vulnerability * Impacts
- Risk Assessment & Risk Mitigation
- Model: *Advanced Persistent Threats (APT)*
- Security Investment Analysis



Attack-Defense Evaluations

- Generation of stealth attack vectors
- Quantification of system impacts
- Evaluation of mitigation schemes

Case Study: Attack on Remedial Action Scheme

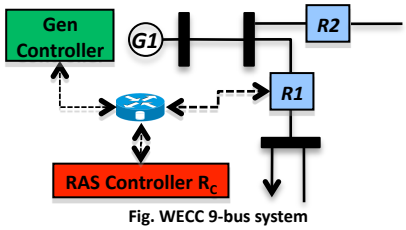


Fig. WECC 9-bus system

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

Industry Partners

SEL Schweitzer Engineering Laboratories · OPAL-RT · RTDS Technologies · SIEMENS · Mu Dynamics · PSERC