PowerCyber: A Remotely Accessible CPS Security Testbed for Smart Grid

Pengyuan Wang, Aditya Ashok, Subramanian Arunachalam, Manimaran Govindarasu

Iowa State University

Motivation & Objective

Motivation

A hardware-in-the-loop testbed provides an economic real-time simulation platform for cyber physical system (CPS) vulnerability & impact analysis, modern CPS security technologies validation and evaluation, and can greatly assist the R&D of novel resilient Wide Area Monitoring, Protection and Control (WAMPAC) functions for smart grid.

Objective

- Construct hybrid CPS testbed with satisfactory performance in terms of of accuracy, scalability and cost.
- Implement possible cyber threats, analyze and evaluate power system vulnerabilities & impacts.
- Develop and test novel countermeasures at both cyber layer and physical layer to validate the efficacy and resiliency.

Testbed Architecture

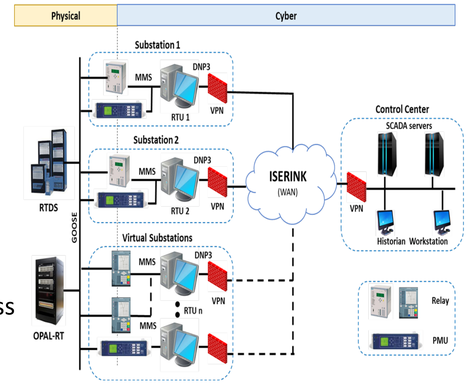
ISU PowerCyber Testbed

Provides a unique cyber-physical integration for bulk power system with high-fidelity and high-scalability.

Critical Components

Physical layer
- RTDS
- Opal-RT simulator

Cyber layer
- Siemens EMS/SCADA
- Relays/PMU
- ISERINK
- Web-based remote access
- Federation potential



Capability

R&D Applications

- 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

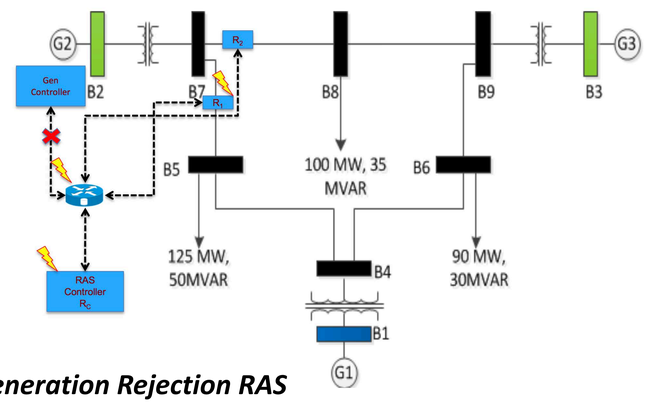
Several Early Users

Organization	Use Case
Pacific Northwest National Lab	CPS security of AGC study and Attack Resilient Control (ARC) design.
accenture	Validating Alert Correlation Engine (as part of Anomaly Detection System) in a realistic ICS environment.
Symantec	Validating Symantec ICS Anomaly-Detection System(ADS) in a SCADA environment
John Hopkins University	Novel IPS design based on PLCICMP and TCP packet features considering varying CPU load levels.
University of Minnesota Duluth	CPS experiment sessions of an EE graduate course.
Grid Security Conference (2015 & 2016)	Utilities employees hands-on the cyber attack and defense practice modules.

CPS Security of WAMPAC

Remedial Action Scheme (RAS)

Coordinated attack Impact analysis



Generation Rejection RAS

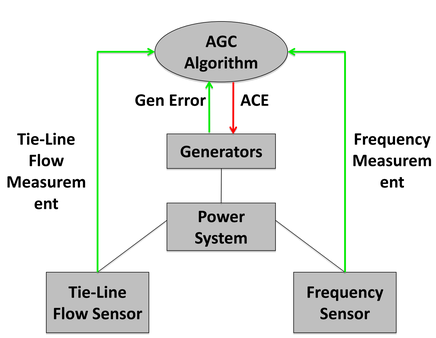
Generation rejection RAS is set up for G2 in IEEE 9-bus system. RAS controller will trigger load shedding to avoid overload when either line 7-8 or line 7-5 goes out of service.

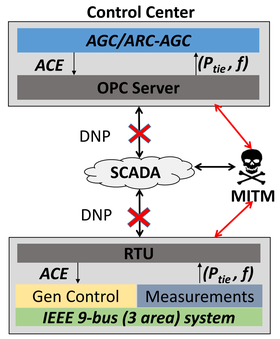
Intelligent Coordinated Attack on RAS

Step1: Sniff plain-text packets opening breaker R1.
Step2: Denial of Service (DoS) attack on the controller or the router.
Step3: Trip line 7-5 with replay attack.

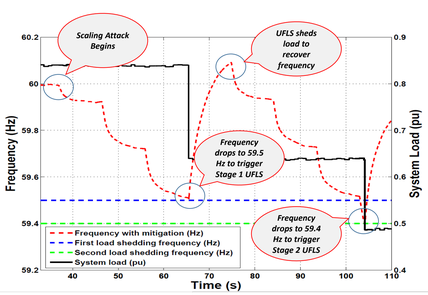
Automatic Generation Control

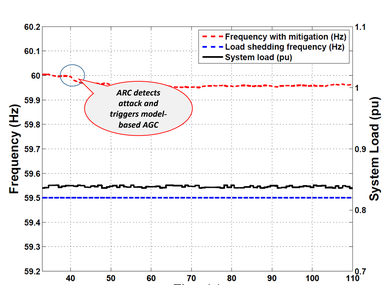
Model-based ARC design





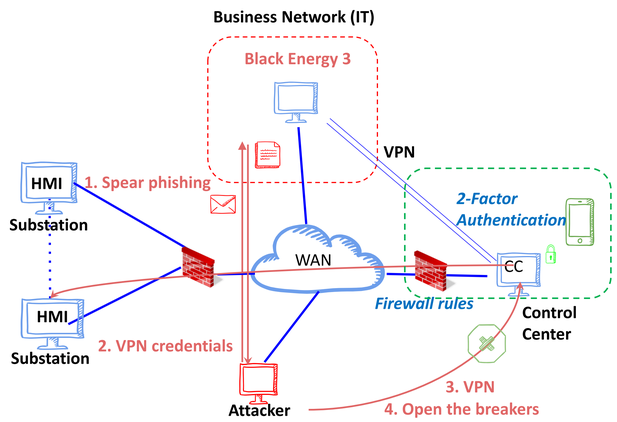
MITM attack Impact and Attack Resilient Control





Ukrainian Attack (2015)

Replication of a real attack



Attack

Step1: Phishing email sent to IT host with VPN capability.
Step2: Reconnaissance and VPN credential theft after getting the reverse shell.
Step3: Launching the attack by VPN into CC and trip breakers.

Defense

VPN with 2-factor authentication, egress filtering, etc.