Cyber-Physical System Security of the Power Grid

Chen-Ching Liu
American Electric Power Professor
Director, Power and Energy Center
Virginia Tech

Sponsored by National Science Foundation, Department of Energy, and Science Foundation Ireland, Murdock Charitable Trust, ESIC Washington State University, State of Washington
CPS Security Research in Power Grids

Vulnerability assessment
- System modeling
- Impact analysis
- Identify weaknesses

Intrusion/Anomaly detection
- Attack simulation/analysis
- Detection approach
- Validation (Testbed)

Mitigation methodology
- Cyber system
- Physical system

Source: Avista
Cyber-Physical System Model

Transmission Operator Layer

Control Center Level at Cyber System Layer

Substation Level at Cyber System Layer

Power System Layer
Impact on Power System - Dynamics

- Cyber-Physical Security Assessment

Impact of the cyber attack is assessed by monitoring the dynamic behavior:

- frequency \[ \beta_j = \beta_{f,j} + \beta_{P,j} + \beta_{U,j} + \beta_{L,j} \]
- bus voltage magnitudes
- current levels on network elements
- loss of loads

It shows how much the operation has moved from the secure condition:

- secure
- insecure
- critical

The most critical attack path is identified based on the attack’s efficiency
Simulation of Cyber-Power Systems

Power systems simulation tool

DIgSILENT power factory

Controls

Measurements

OPC (OLE for Process Control)

Controls

Resulting impact from simulator

Result data

Input data

MATLAB

Substation ICT networks and IADS

Attack similarity Impact analysis
Potential Threats in a Substation Based on IEC 61850

- **Compromise user-interface** (Staion Level)
- **Gain access to bay level devices** (Bay Level)
- **Modify GOOSE message** (Process Level)
- **Generate fabricated analog values** (Process Level)

Diagram:

- **User-interface** (Station Level)
- **GPS**
- **Merging Unit**
- **Actuator**
- **Circuit Breaker**
- **CT and VT**

IEPs, Relay, PMU, User-interface, GPS, Change device settings
IEEE 39 Bus System

**Protection IED: Circuit Breaker**

- Relay Status: Normal
- Status: [Closed]
- Circuit Breaker Status: CLOSED

**Protection IED: Overcurrent Relay**

- Operation: Normal
- Current Values [A] RMS:
  - la: 5.02
  - lb: 5.01
  - lc: 5.03
- Setting Values [A]:
  - Instantaneous: 125
  - Time overcurrent: 30
- Circuit Breaker Status: CLOSED

Normal status
Sequential attacks – Sub # 6 → 12 → 15 → 28 → 36 → 33 → 34
Sequential attacks – Sub # 6 → 12 → 15 → 28 → 36 → 33 → 34
Sequential attacks – Sub # 6 → 12 → 15 → 28 → 36 → 33 → 34
Sequential attacks – Sub # 6 → 12 → 15 → 28 → 36 → 33 → 34
Sequential attacks – Sub # 6 → 12 → 15 → 28 → 36 → 33 → 34
Sequential attacks – Sub # 6 → 12 → 15 → 28 → 36 → 33 → 34
HMI
HMI

Anomaly Detection System

GOOSE
SMV
CB

User-interface
Firewall

Single Line Overview
Alarm Logs
Event Logs
Acknowledgement

Anomaly Indicators
Anomaly Attempt
Change File System
Change System Status
GOOSE
SMV
Detected Anomaly
1575

(Images of equipment and settings related to the HMI and anomaly detection system)
Coordinated Cyber Attack Detection System (CCADS)

- Abnormal Behavior: 0.8257
- Criticality Relation: 0.9701
- Geographical Relation: 0.8165

Relation Correlation System: 0.9882

Coordinated Cyber Attack Warning: Threshold 0.9

Similarity index

User defined threshold value

Compromised substations
Coordinated Cyber Attack Detection System (CCADS)
Frequency/Voltage Responses to Attacks w/o Intrusion Detection System
Further Information


