Cyber-Physical System Security of the Power Grid

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

Sponsored by U.S. National Science Foundation and Science Foundation Ireland, Murdock Charitable Trust, ESIC Washington State University, State of Washington
Bradley Dept. of Electrical & Computer Engineering

- Tenured/tenure-track faculty: 79
- Students: 1,400 BS; 210 MS; 350 PhD
- Graduates: 54 PhDs; 130 MS/MEng; 267 BS awarded past academic year
- Ranked 10th for research expenditures by NSF
- Fellows: IEEE 31; other societies 9
- National Academy of Engineering (NAE): 4
- NSF CAREER Awards: 20; DoD YIP Awards: 6; Sloan Research Fellow: 1
- US News & World Report rankings
  - Graduate programs (2018): EE 18th; CPE 17th
  - Undergraduate programs (2017): EE 13th; CPE 15th
ECE Locations

Main Campus
• Undergraduate programs
• Graduate programs
• Research

Blackburg, VA

Arlington, VA
Falls Church, VA

12 faculty at National Capital Region
• Primarily graduate programs
• Research

Whittemore Hall
Durham Hall
Torgersen Hall
VT Research Center (Arlington)
Northern Virginia Center (Falls Church)
Center for Power & Energy (CPE)

- Founded by A. Phadke in 1986
- **Original members:** A. Phadke; L. Mili; R. Broadwater; S. Rahman; K. Tam; Y. Liu; and J. DeLaRee

- 1988: First Phasor Measurement Unit (PMU)
- 2002: Frequency Monitoring Network (FNET)
- 2008: A. Phadke and J. Thorp awarded Benjamin Franklin Medal in EE
- 2013: PMU-only three-phase state estimator in Dominion Virginia Power
CPE Core Faculty

Chen-Ching Liu
Director & AEP Professor
- Distribution systems, cyber security of the grid
- Industry software for system restoration: EPRI (T), PNNL (D)

Mona Ghassemi
Assistant Professor

Jaime De La Ree
Associate Professor & Assistant Dept. Head

Lamine M. Mili
Professor (NVC)

Vassilis Kekatos
Assistant Professor
- Optimization and learning of smart grids

Robert Broadwater
Professor

Saifur Rahman
Joseph Loring Professor (VT-ARC)
- Energy efficiency and sensor integration
- DoE BEMOSS Platform: President of IEEE PES

Virgilio A. Centeno
Associate Professor

Mona Ghassemi
Assistant Professor
Cyber Attack in Ukraine’s Power System

• Attack on Ukraine’s power grid
  ❑ December 23, 2015.
  ❑ Malware installation.
  ❑ Falsify SCADA data injection.
  ❑ Flood attack on telephone system.
  ❑ Trip circuit breakers in multiple substations.

• Results
  ❑ Over 225,000 customers experienced power outage.
Power Grid with ICT
Critical Cyber Assets

Critical Cyber Assets in Power infrastructure

- Energy Management System (EMS) in Control Center
- Distribution Management System (DMS)
- Process Control System (Power Plants)
- Substation Automation System (SAS)
Evolution of SCADA Systems

Evolved through generations

- Monolithic
- Distributed
- Networked
Escalating Cyber Security Factors

- Adoption of standardized technologies with known vulnerabilities
- Connectivity of control systems to other networks
- Constraints on use of existing security technologies and practices
- Insecure remote connections
- Widespread availability of technical information about control systems
Access Points in Control Networks

- Virtual Private Network (VPN)
- Dial-up Networks
- Wireless Networks
- Any Remote Logon Programs
- Backdoor Access - Trojan Horse
Intrusion Tools

- War Dialing
- Scanning
- Traffic Sniffing
- Password Cracking
- Stuxnet
- Ukraine
# Supervisory Control And Data Acquisition (SCADA)

<table>
<thead>
<tr>
<th>Sectors</th>
<th>Electric Power</th>
<th>Natural Gas Pipelines, Process Control Systems</th>
<th>Transportation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Transmission, Distribution, Substation Network Monitoring) Wind Farms</td>
<td>Gas Pipeline, Chemical, Oil and Gas, Power Plants</td>
<td>Roadway, Rail System, Space and Air Traffic</td>
</tr>
<tr>
<td>Example Protocols</td>
<td>ICCP / DNP3i / Modbus over TCP/IP / IEC870-5-101/104 / IEC 61850</td>
<td>Fieldbus or Profibus</td>
<td>Cellular Digital Packet Data Network and Global Positioning System</td>
</tr>
<tr>
<td>Framework</td>
<td>Data Polling Acquisition &amp; Control / Automation Are Configured for Interlocking and Protection Scheme</td>
<td>Automation by Programmable Logic Controller (PLC)</td>
<td>Ensuring Associated Tasks with Given Function, Satisfying System Performance in Centre</td>
</tr>
<tr>
<td>Control Variables</td>
<td>Switching Devices</td>
<td>Valve, Pump</td>
<td>Controls of Roadway Access and Intersection Devices</td>
</tr>
</tbody>
</table>
Cyber Security Standards NERC CIP 002-009

- Critical asset identification (e.g. RTU, which support the reliable operation of a power system.)
- Security management controls (e.g. How to manage the authentication, card or password, or both.)
- Personnel training (e.g. Contractors and vendor must be authorized to gain access (cyber and physical), and training staff on security awareness.)
- Electronic security perimeter (e.g. Periphery to protect all the cyber asset within.)
- Physical security of critical cyber assets (e.g. Control policies on people who are authorized to have access to the critical cyber assets.)
- System security management (e.g. Monitoring system events)
- Incident reporting and response planning (e.g. Report to related authorities if necessary)
- Recovery plans for critical cyber assets (e.g. When threat is over, recover the system and enhance the control policies)
Cyber Security Monitoring

- Impact Analysis
- Anomaly Detection
- Real-Time Monitoring
- Power System
- Mitigation
- Control Center
- ICT
- Substation
Cyber Systems in Power Infrastructure

Other Corporate Intranets

Primary Control Center Network
- User Interfaces
- Dispatcher Training Simulators
- Modem
- Application Servers
- SCADA Servers
- Database Servers
- Firewall
- Router

Secondary Control Center Network
- Modem
- Firewall
- Data Concentrator
- Dispatcher Training Simulators

Substation Network
- User Interfaces
- Modem
- Data Concentrator
- Firewall
- Router

Frame Relay Network / Radiowave / Dedicated Line

Remote Access Network through Dial-up, VPN, or Wireless

Corporate WAN

Vendor Personnel or Site Engineers

Breaker
- Busbar
- Transformer
- Feeder

Transmission line
System Vulnerability

- A system is defined as the wide area interconnected, IP-based computer communication networks linking the control center and substations-level networks.
- System vulnerability is the maximum vulnerability level over a set of scenarios represented by I.

\[ V_S = \max(V(I)) \]
An intrusion scenario consists of the steps taken by an attempted attack from a substation-level network.

Substation-level networks in a power system:
- substation automation systems
- power plant control systems
- distribution operating centers

Scenario vulnerability is defined by:

\[ V(I) = \{V(i_1), V(i_2), K, V(i_K)\} \]

where \( K \) is the number of intrusion scenarios to be evaluated.
Access Point Vulnerability

- Access point provides the port services to establish a connection for an intruder to penetrate SCADA computer systems

- Vulnerability of a scenario \( i \), \( V(i) \), through an access point is evaluated to determine its potential damage

- Scenario vulnerability - weighted sum of the potential damages over the set \( S \).

\[
V(i) = \sum_{j \in S} \pi_j \times \gamma_j
\]

where \( \pi_j \) is the steady state probability that a SCADA system is attacked through a specific access point \( j \), which is linked to the SCADA system. The damage factor, \( \gamma_j \), represents the level of damage on a power system when a substation is removed.
Password Model

- Intrusion attempt to a machine
  - A solid bar - transition probability
  - An empty bar - processing execution rate that responds to the attacker

- Account lockout feature, with a limited number of attempts, can be simulated by initiating the N tokens (password policy threshold).

\[
p_{i}^{pw} = \frac{f_{i}^{pw}}{N_{i}^{pw}}
\]
**Firewall Model**

- **Firewall model**
  - Denial or access of each rule
  - Malicious packets traveling through policy rule \( j \) on each firewall \( i \) is taken into account.

\[
p_{i,j}^{fp} = \frac{f_{i,j}^{fp}}{N_{i,j}^{fp}}
\]

- probability of malicious packets traveling through a firewall rule

\[
p_{i}^{fr} = \frac{f_{i}^{fr}}{N_{i}^{fr}}
\]

- probability of the packets being rejected

- denotes the frequency of malicious packets through the firewall rule

- total record of firewall rule \( j \).

- the number of rejected packets

- denotes the total number of packets in the firewall logs

- Malicious packets passed through Firewall A (terminal 2)

- Intrusion Attempts (terminal 1)

- Deny Rule 1

- Rule 2

- Rule \( n \)
Construction of Cyber-Net Based on Substation with Load and Generator
Impact Factor Evaluation

- Impact factor for the attack upon a SCADA system is

\[ \gamma = \left( \frac{P_{LOL}}{P_{Total}} \right)^{L-1} \]

- Loss of load (LOL) is quantified for a disconnected substation

- To determine the value of L, one starts with the value of L=1 at the substation and gradually increases the loading level of the entire system without the substation that has been attacked.

- Stop when power flow fails to converge (System is considered unstable)
## Impact Factor Evaluation for IEEE 30-Bus System

### Impact Factor for Each Substation

<table>
<thead>
<tr>
<th>Sub.</th>
<th>Associated Buses</th>
<th>LOL(MW)</th>
<th>L</th>
<th>$\gamma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>.3</td>
<td>2.5</td>
<td>.0016</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>21.7</td>
<td>1.8</td>
<td>.1769</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>2.4</td>
<td>2.5</td>
<td>.0014</td>
</tr>
<tr>
<td>4</td>
<td>4, 12, 13</td>
<td>18.8</td>
<td>1.4</td>
<td>.3971</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>0</td>
<td>2.5</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>6, 9, 10, 11</td>
<td>5.8</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>22.8</td>
<td>2.8</td>
<td>.0222</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>30</td>
<td>3.6</td>
<td>.0083</td>
</tr>
<tr>
<td>9</td>
<td>14</td>
<td>6.2</td>
<td>2.9</td>
<td>.0015</td>
</tr>
<tr>
<td>10</td>
<td>15</td>
<td>8.2</td>
<td>3</td>
<td>.0019</td>
</tr>
<tr>
<td>11</td>
<td>16</td>
<td>3.5</td>
<td>2.6</td>
<td>.0017</td>
</tr>
<tr>
<td>12</td>
<td>17</td>
<td>9</td>
<td>2.9</td>
<td>.0031</td>
</tr>
<tr>
<td>13</td>
<td>18</td>
<td>3.2</td>
<td>3.1</td>
<td>.0002</td>
</tr>
<tr>
<td>14</td>
<td>19</td>
<td>9.5</td>
<td>2.9</td>
<td>.0034</td>
</tr>
<tr>
<td>15</td>
<td>20</td>
<td>2.2</td>
<td>2.9</td>
<td>.0002</td>
</tr>
<tr>
<td>16</td>
<td>21</td>
<td>17.5</td>
<td>2.6</td>
<td>.0222</td>
</tr>
<tr>
<td>17</td>
<td>22</td>
<td>0</td>
<td>2.2</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>23</td>
<td>3.2</td>
<td>2.7</td>
<td>.0010</td>
</tr>
<tr>
<td>19</td>
<td>24</td>
<td>8.7</td>
<td>2.9</td>
<td>.0029</td>
</tr>
<tr>
<td>20</td>
<td>25</td>
<td>0</td>
<td>2.8</td>
<td>0</td>
</tr>
<tr>
<td>21</td>
<td>26</td>
<td>3.5</td>
<td>2.8</td>
<td>.0008</td>
</tr>
<tr>
<td>22</td>
<td>27, 28</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>23</td>
<td>29</td>
<td>2.4</td>
<td>2.8</td>
<td>.0004</td>
</tr>
<tr>
<td>24</td>
<td>30</td>
<td>10.6</td>
<td>2.8</td>
<td>.0056</td>
</tr>
</tbody>
</table>
Modeling Integrated Cyber-Power System

• **Methodology for CPS modeling of power systems**
  – Develop the ICT model of SCADA system
  – Integrate power grid model with ICT model for SCADA and grid control hierarchy
  – Dynamics of a power grid and its data infrastructure are combined

• **CPS tool used for assessment of SCADA communication performance**
  – Plan SCADA and ICT systems for power grids

• **CPS tool used for cyber security assessment in co-simulation environment**
  – Model cyber attacks and assess CPS security
    • Simulate cyber attacks at the cyber system layer
    • Perform impact analysis at the power system layer
    • Compute impact indices and attack efficiencies to disrupt power grid operation
Cyber-Physical System Model
Cyber-Physical System Tool

Cyber System and Transmission Operator Layers
- Transmission Operator's Console
- Real-time Database
- SCADA Mimics
- OPC Client State, Control Variables
- Matrikon OPC Simulation Server
- MATLAB Simulink, SimEvents, OPC Toolboxes
- OPC Client State, Control Variables
- SIEMENS Spectrum Power TG, SICAM PAS
- DIgSILENT PowerFactory OPC Client State, Control Variables
- Power Grid Static and Dynamic Models

Cyber Attacks
& Impact Analysis

Real-Time Grid Supervision & Control, EMS Tools
SCADA Performances
Communication Security
Intrusion into a Substation Network

Frame Relay Network / Radiowave / Dedicated Line

Remote Access Network through Dial-up, VPN, or Wireless

Other Corporate Intranets

Corporate WAN

Primary Control Center Network

Secondary Control Center Network

Substation Network
Vulnerabilities of Substations

- Control centers rely on substations and communications to make decisions
- Substations are a critical infrastructure in the power grid (relays, IEDs, PMUs)
- Remote access to substation user interface or IEDs for maintenance purposes
- Unsecured standard protocol, remote controllable IED and unauthorized remote access
- Some IED and user-interface have available web servers and it may provide a remote access for configuration and control with default passwords
- Well coordinated cyber attacks can compromise more than one substation – it may become a multiple, cascaded sequence of events
Potential Threats in a Substation Based on IEC 61850

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

- **IED**
- **Relay**
- **PMU**
- **User-interface**
- **GPS**
- **Change device settings**
- **Actuator**
- **Circuit Breaker**
- **Merging Unit**
- **CT and VT**
Anomaly Detection at Substations
Integrated Anomaly Detection System

Network-based ADS module:
- Predefined logics
- Security constraints
- Alarm data

Host-based ADS module:
- Temporal anomaly detection
- Intrusion attempt
- Change of IED setting
- Alarm data
- Measurement difference

Packet filtering module
- GOOSE

Packet parser module
- SV

Human machine Interface (HMI) module

Event logs
- Normal operation

Shared memory
- ADS Data

Alarm logs
- Violation

Substation ICT network

User-interface, IEDs, and firewall

System and security logs
Host-Based Anomaly Detection

- Detection of temporal anomalies is performed by comparing consecutive row vectors representing a sequence of time instants

\[ V_{\Omega}^{h(i)} = \frac{\sum_{j=1}^{n} |\Omega(i,j) - \Omega(i+1,j)|}{n}, \quad i = 1, \ldots, 6, \]

- If a discrepancy exists between two different periods (rows, 10 seconds), the anomaly index is a number between 0 and 1

- A value of 0 implies no discrepancy whereas 1 indicates the maximal discrepancy

Host-based anomaly indicators
- \( \psi^a \) (intrusion attempt on user interface or IED)
- \( \psi^{cf} \) (change of the file system)
- \( \psi^{cs} \) (change of IED critical settings)
- \( \psi^o \) (change of status of breakers or transformer taps)
- \( \psi^m \) (measurement difference)

<table>
<thead>
<tr>
<th>Substation A</th>
</tr>
</thead>
<tbody>
<tr>
<td>( t_1 )</td>
</tr>
<tr>
<td>( t_2 )</td>
</tr>
<tr>
<td>( t_3 )</td>
</tr>
<tr>
<td>( \Omega = t_4 )</td>
</tr>
<tr>
<td>( t_5 )</td>
</tr>
<tr>
<td>( t_6 )</td>
</tr>
<tr>
<td>( t_7 )</td>
</tr>
</tbody>
</table>
At 10:20:000, there is no anomaly so $t_1$ is $[0 \ 0 \ 0 \ 0 \ 0]$.
- At 10:30:000, ADS detects a wrong password attempt to IED 1 so $t_2$ is $[1 \ 0 \ 0 \ 0 \ 0]$.
- At 10:40:000, ADS detects an unauthorized file change to the user-interface so $t_3$ is $[1 \ 1 \ 0 \ 0 \ 0]$.
- At 10:50:000, there is no change so $t_4$ is $[1 \ 1 \ 0 \ 0 \ 0]$.
- At 11:00:000, there is no change so $t_5$ is $[1 \ 1 \ 0 \ 0 \ 0]$.
- At 11:10:000, ADS detects two anomalies, unauthorized setting change to IED 2 and unauthorized tap change to transformer 1 so $t_6$ is $[1 \ 1 \ 1 \ 1 \ 0]$.
- At 11:20:000, there is no change so $t_7$ is $[1 \ 1 \ 1 \ 1 \ 0]$.
Substation Cyber Security Testbed

Integrated Anomaly Detection System

- SCADA: Supervisory Control and Data Acquisition
- DNP3: Distributed Network Protocol 3
- VPN: Virtual Private Network
- MMS: Manufacturing Message Specification
- GOOSE: Generic Object Oriented Substation Events
- SV: Sampled Value
- IED: Intelligent Electronic Device
## Consequence of GOOSE Based Attack

<table>
<thead>
<tr>
<th>Action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnect Ethernet cable from IED</td>
<td>Lost availability of IED</td>
</tr>
<tr>
<td>Send normal control</td>
<td>Open CB</td>
</tr>
<tr>
<td>Replay attack</td>
<td>Open CB</td>
</tr>
<tr>
<td>Modify sequence &amp; state number</td>
<td>Warning occurred at CB</td>
</tr>
<tr>
<td>Modify transferred time</td>
<td>Warning occurred at CB</td>
</tr>
<tr>
<td>Modify GOOSE control data</td>
<td>Open CB</td>
</tr>
<tr>
<td>Denial of Service attack</td>
<td>Lost availability of CB</td>
</tr>
<tr>
<td>Generate GOOSE control data</td>
<td>Open CB</td>
</tr>
</tbody>
</table>
### Consequence of SV Based Attack

<table>
<thead>
<tr>
<th>Action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnect Ethernet cable from MU</td>
<td>Lost availability of MU</td>
</tr>
<tr>
<td>Increase measured values</td>
<td>Open CB</td>
</tr>
<tr>
<td>Replay attack</td>
<td>Open CB</td>
</tr>
<tr>
<td>Modify counter number</td>
<td>Warning occurred at IED</td>
</tr>
<tr>
<td>Modify SMV dataset</td>
<td>Warning occurred at IED</td>
</tr>
<tr>
<td>Denial of Service attack</td>
<td>Lost availability of IED</td>
</tr>
<tr>
<td>Generate SMV data</td>
<td>Open CB</td>
</tr>
</tbody>
</table>
System Integration

Power systems simulation tool

DIgSILENT power factory

Controls

Measurements

OPC (OLE for Process Control)

Controls

Resulting impact from simulator

Input data

Result data

MMS-EASE lite

Substation ICT networks and IADS

MATLAB

Attack similarity Impact analysis
IEEE 39 Bus System

Normal status
Sequential attacks – Sub # $6 \rightarrow 12 \rightarrow 15 \rightarrow 28 \rightarrow 36 \rightarrow 33 \rightarrow 34$
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
Sequential attacks – Sub # 6 → 12 → 15 → 28 → 36 → 33 → 34
IEEE 39 Bus System (DIgSILENT)

1. Bus 6
2. Bus 12
3. Bus 15
4. Bus 28
5. Bus 36
6. Bus 33
7. Bus 34

Gen 1
Gen 2
Gen 3
Gen 6
Gen 9
Gen 10

Without ADS - Blackout
Sequential attacks with ADS
HMI
Anomaly Detection System
IEEE 39 Bus System (DIgSILENT)
Coordinated Cyber Attack
GUI of CCADS

- Abnormal Behavior: 0.8257
- Criticality Relation: 0.9701
- Geographical Relation: 0.8165
- Relation Correlation System: 0.9892
- Coordinated Cyber Attack Warning: Threshold 0.9

Similarity index
User defined threshold value
Compromised substations
Simulation of Power System
Intrusion Detection System
Further Information


Further Information (Conti)
