Electric Energy System Cybersecurity: An Overview

Sakis Meliopoulos
Georgia Power Distinguished Professor
ECE, Georgia Tech
Contents

• Background
• Electric Energy Systems – Cyber Infrastructure
• Vulnerabilities
• Cybersecurity Standards – present practice
• Advanced Cybersecurity Systems
  – State and Model Based Detection Systems
  – Context Based Authentication
• Demonstrations
• Concluding Remarks
The Ever Increasing Attack Surface of the electric Energy Grid
Basic Components of the Electric Energy Grid Cyberspace

Bulk Power System

Distribution/Customer Level

Need to utilize customer flexibility drives to the concept of IoTE
Vulnerabilities
Hackers can:
- Cause severe disruptions to electric grid
- Cause severe damage to major electric grid components
- Manipulate voltages at customers causing failures

Example 1: GPS Spoofing
Electric energy systems depend on GPS synchronized measurements. Spoofing GPS receivers can lead to relay mis-operations and compromised operational security

Example 2: AURORA Attack/Controller Attack
Closing of generator breaker while generator is at standstill

Example 3: Distribution System Controller Attack
Access controllers of transformers, reclosers, cap banks, and manipulate voltages at customers causing massive appliance failures
### IRIG-B Frame Information Encoding

<table>
<thead>
<tr>
<th>Number of Bits</th>
<th>Encoding</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>BCD</td>
<td>Seconds of Minute (0-59)</td>
</tr>
<tr>
<td>7</td>
<td>BCD</td>
<td>Minutes of Hour (0-59)</td>
</tr>
<tr>
<td>6</td>
<td>BCD</td>
<td>Hours of Day (0-24)</td>
</tr>
<tr>
<td>10</td>
<td>BCD</td>
<td>Days of Year (0-366)</td>
</tr>
<tr>
<td>9</td>
<td>BCD</td>
<td>Year (last two digits)</td>
</tr>
<tr>
<td>18</td>
<td>Binary</td>
<td>Control Bits</td>
</tr>
<tr>
<td>17</td>
<td>Binary</td>
<td>Seconds of Day (0-86399)</td>
</tr>
</tbody>
</table>
Satellite Elevation & Elevation Mask
Satellite Position/Speed and Receiver Position/Speed

- \(x_1, y_1, z_1\)
- \(\dot{x}_1, \dot{y}_1, \dot{z}_1\)
- \(x_2, y_2, z_2\)
- \(\dot{x}_2, \dot{y}_2, \dot{z}_2\)
- \(x_3, y_3, z_3\)
- \(\dot{x}_3, \dot{y}_3, \dot{z}_3\)
- \(x_4, y_4, z_4\)
- \(\dot{x}_4, \dot{y}_4, \dot{z}_4\)
- \(x_5, y_5, z_5\)
- \(\dot{x}_5, \dot{y}_5, \dot{z}_5\)

Earth

GPS Receiver
Example 2: Controller Attack
Hacker gains access to distribution system communications

Distribution voltage control uses IEDs to control:

- Load Tap Changer transformers
- Voltage Regulators
- Pole-top capacitor banks

A Successful Hacker can enter the communications network and drive all controls to maximum. In a typical system this may lead to 30% overvoltage causing widespread transformer failures and customer equipment failures (air-conditioners, stereos, refrigerators, etc.)

QUESTION: How secure are distribution system communications networks?
Example Controller Attack
Example 1: AURORA Attack
Closing of generator breaker while generator is at standstill
Standards
• IEEE, CIGRE, NIST, NERC, FERC all are involved in developing cyber security standards

• NIST Cyber Security Framework (v 1.0 in Feb 2014)

• NERC Critical Infrastructure Protection (CIP) Standards
Example Cyber Security Standards

IEEE Standards
- IEEE Std 1686 “IEEE Standard for Intelligent Electronic Devices (IEDs) Cyber Security Capabilities”
- IEEE C37.240 “Standard for Cyber Security Requirements for Substation Automation, Protection and Control Systems” (under development)

IEC Standards
- IEC 62351

NERC Standards
- NERC Critical Infrastructure Protection (CIP) CIP-002 to CIP-009

NIST
IEC Series of Standards

IEC 62351-1: Introduction

IEC 62351-2: Glossary

IEC 62351-3: Profiles Including TCP/IP

IEC 62351-4: Profiles Including MMS

IEC 62351-5: IEC 60870-5 and Derivatives

IEC 62351-6: IEC 61850

IEC 60870-6 TASE.2

IEC 61850-8-1 MMS Profile

IEC 60870-5-104 TCP/IP

IEC 60870-5-101, 102 and 103

IEC 61850-8-1 GOOSE Profile

IEC 61850-9-2 SMV Profile

IEC 62351 Part 7: NSM Data Objects for Network and System Management
Security Monitoring Architecture, Using NSM Data Objects

Legend:
- Clients
- Servers
- Other
- Firewall
  - NSM Data Objects
  - Intrusion Detection System (IDS)
IEEE Std C37-240

IEEE Standard

Cybersecurity Requirements for Substation Automation, Protection, and Control Systems.

Effectively maps NISTIR 7628 into the substation system.
## IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities

### Table A.1—Table of compliance

<table>
<thead>
<tr>
<th>Clause number</th>
<th>Clause/subclause title</th>
<th>Status</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>IED cyber security features</td>
<td>Acknowl</td>
<td></td>
</tr>
<tr>
<td>5.1</td>
<td>Electronic access control</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.1.2</td>
<td>Password defeat mechanisms</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.1.3</td>
<td>Number of individual users</td>
<td>Exceed</td>
<td>Product provides for 25 individual ID/password combinations</td>
</tr>
<tr>
<td>5.1.4</td>
<td>Password construction</td>
<td>Exception</td>
<td>Upper and lower case letters are interchangeable. Non-alphanumeric characters cannot be used in password</td>
</tr>
<tr>
<td>5.1.5</td>
<td>IED access control</td>
<td>Acknowl</td>
<td></td>
</tr>
<tr>
<td>5.1.5.1</td>
<td>Authorization levels by password</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.1.5.2</td>
<td>Authorization using role-based access control (RBAC)</td>
<td>Exceed</td>
<td>Product provides six user-defined roles</td>
</tr>
<tr>
<td>5.1.6</td>
<td>IED main security functions</td>
<td>Acknowl</td>
<td></td>
</tr>
<tr>
<td>5.1.6 a)</td>
<td>View data</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.1.6 b)</td>
<td>View configuration settings</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.1.6 c)</td>
<td>Force values</td>
<td>Exception</td>
<td>Feature not supported on this product</td>
</tr>
<tr>
<td>5.1.6 d)</td>
<td>Configuration change</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.1.6 e)</td>
<td>Firmware change</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.1.6 f)</td>
<td>ID password or RBAC management</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.1.6 g)</td>
<td>Audit trail</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.1.7</td>
<td>Password display</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.1.8</td>
<td>Access timeout</td>
<td>Exception</td>
<td>Timeout period is set by a jumper on the main board. Possible selections are 1 min, 5 min, 10 min, 30 min, and 60 min</td>
</tr>
<tr>
<td>5.2</td>
<td>Audit trail</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.2</td>
<td>Storage capability</td>
<td>Exceed</td>
<td>Audit trail supports 4096 events before overwrite</td>
</tr>
<tr>
<td>5.2.3</td>
<td>Storage record</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.3 a)</td>
<td>Event record number</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.3 b)</td>
<td>Time and date</td>
<td>Exceed</td>
<td>User can define the format of the date</td>
</tr>
<tr>
<td>5.2.3 c)</td>
<td>User identification</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.3 d)</td>
<td>Event type</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.4</td>
<td>Audit trail event types</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.4 a)</td>
<td>Log in</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.4 b)</td>
<td>Manual log out</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.4 c)</td>
<td>Timed log out</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.4 d)</td>
<td>Value forcing</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.4 e)</td>
<td>Configuration access</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.4 f)</td>
<td>Configuration change</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.4 g)</td>
<td>Firmware change</td>
<td>Exception</td>
<td>Firmware changes are not captured in the audit trail record</td>
</tr>
</tbody>
</table>
IEEE Standard 1686

IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities

<table>
<thead>
<tr>
<th>Clause number</th>
<th>Clause/Subclause Title</th>
<th>Status</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.4 i)</td>
<td>Password deletion</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.4 j)</td>
<td>Audit log access</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.4 k)</td>
<td>Time/date change</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.2.4 l)</td>
<td>Alarm incident</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.3</td>
<td>Supervisory monitoring and control</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.3.2</td>
<td>Events</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.3.3</td>
<td>Alarms</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.3.3 a)</td>
<td>Unsuccessful login attempt</td>
<td>Exception</td>
<td>Alarm is set after six unsuccessful attempts within a 5-min period</td>
</tr>
<tr>
<td>5.3.3 b)</td>
<td>Reboot</td>
<td>Exception</td>
<td>A specific alarm for a reboot is not available. However, user can deduce that a reboot has taken place by examining the DNP3.0 initialization bit being set follows by a DNP3.0 request for time.</td>
</tr>
<tr>
<td>5.3.3 c)</td>
<td>Attempted use of unauthorized configuration software</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.3.3 d)</td>
<td>Invalid configuration or firmware download</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.3.3 e)</td>
<td>Unauthorized configuration or firmware file</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.3.3 f)</td>
<td>Time signal out of tolerance</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.3.3 g)</td>
<td>Invalid field hardware changes</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.3.4</td>
<td>Alarm point change detect</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.3.5</td>
<td>Event and alarm grouping</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.3.6</td>
<td>Supervisory permissive control</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.4</td>
<td>IED cyber security features</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.4.1</td>
<td>IED functionality compromise</td>
<td>Comply</td>
<td>Download of configuration will disable all other operations during the period of download</td>
</tr>
<tr>
<td>5.4.2</td>
<td>Specific cryptographic features</td>
<td>Acknowledge</td>
<td></td>
</tr>
<tr>
<td>5.4.2 a)</td>
<td>Webserver functionality</td>
<td>Comply</td>
<td>Feature not offered in this product</td>
</tr>
<tr>
<td>5.4.2 b)</td>
<td>File transfer functionality</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.4.2 c)</td>
<td>Text-oriented terminal connections</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.4.2 d)</td>
<td>SNMP network management</td>
<td>Exception</td>
<td>SNMPv2 implemented in this product</td>
</tr>
<tr>
<td>5.4.2 e)</td>
<td>Network time synchronization</td>
<td>Exception</td>
<td>IEEE Std C37.238 implemented in this product</td>
</tr>
<tr>
<td>5.4.2 f)</td>
<td>Secure tunnel functionality</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.4.3</td>
<td>Cryptographic techniques</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.4.4</td>
<td>Encrypting serial communications</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.4.5</td>
<td>Protocol-specific security features</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.5</td>
<td>IED configuration software</td>
<td>Acknowledge</td>
<td></td>
</tr>
<tr>
<td>5.5.1</td>
<td>Authentication</td>
<td>Exception</td>
<td>Feature not supported</td>
</tr>
<tr>
<td>5.5.2</td>
<td>Digital signature</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.5.3</td>
<td>ID/password control</td>
<td>Exception</td>
<td>Passwords can be viewed in the configuration by someone with Supervisor Level Authority</td>
</tr>
<tr>
<td>5.5.4</td>
<td>ID/password controlled features</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.5.4.1</td>
<td>View configuration data</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.5.4.2</td>
<td>Change configuration data</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.5.4.2 a)</td>
<td>Full access</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.5.4.2 b)</td>
<td>Change tracking</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.5.4.2 c)</td>
<td>Use monitoring</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.5.4.2 d)</td>
<td>Download to IED</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.6</td>
<td>Communications port access</td>
<td>Comply</td>
<td></td>
</tr>
<tr>
<td>5.7</td>
<td>Firmware quality control</td>
<td>Comply</td>
<td></td>
</tr>
</tbody>
</table>
Typical Present Practice

• RADIUS is popular in the electric energy sector.
• RADIUS is a client/server protocol that runs in application layer, using UDP as transport.
• Clients are network access servers—such as wireless access points, 802.1X-capable switches, virtual private network (VPN) servers, and dial-up servers

It serves three purposes:

1. Authenticate users or devices before granting access to network and devices
2. Authorize users or devices for specific network services
3. Account for usage of services
Typical Present Practice

- Internet Protocol Security (IPSec)
- Confidentiality – encryption of data exchanges between substations.
- Integrity – routers at each end of communications (checksum or hush value of data)
- Authentication (signatures and certificates)
- Provides interoperable, high quality, cryptographically-based security for IPv4 and IPv6
- Transparent to applications
- Internet Key Exchange (IKE)
Need More... New Approaches
Data Flow / Applications

- PT
- CT
- Fiber
- UGPSSM
- Breaker
- Data Rate
- 10 ks/s
- Medium: 240 s/s
- Low: 1 s/s
- PQ Analysis
- Process Bus
- IED
- Station Bus 1
- Analog, Status, Commands
- Analog, Status, Commands
- Command Capture Simulation & Authentication
- Signature, Anomaly, & Specification Detection
- Phasors
- Speed
- High
- Medium
- Low
- Data Type
- Sampled Data
- Processed

Cybersecurity Lecture Series
August 23, 2019
State and Model Tracking Based Approaches
Minimize/Eliminate False Positives

"Normal" Operating Conditions

Upon Start of an Event:
- Power System Disturbance
  - Use Available Controls
- Cyber Attack
  - Identify Compromised Device(s)
  - Quarantine Compromised Device(s)

Event Aftermath
- Sanitize Affected Device
- Restore

Track Operating State, Detect Abnormalities
Root Cause Event Analysis, Identify Compromised Devices

Dynamic State Estimation

Merging System
(Sensors, Instrumentation Channels, A/D Conversion)

Physical System
Physically Based Integrated Physical and Cyber System co-Model (PB-PCcoM)

The physical power system (a substation PC co-model is shown) is modeled in terms of its physical construction (3-phase breaker-oriented); the cyber system consisting of relays, instrumentation, communications and human interfaces is integrated with the physical system. Any changes in the physical system propagate to the cyber system and any command at the cyber layer is transmitted to the physical system. This co-modeling approach was introduced 30 years ago before cyber security was a concern.

The integrated model enables co-simulation and evaluation of the complex interactions between the two systems.

Most importantly enables (1) immediate detection and blockage of adversary data and (2) context based authentication or blockage of commands via the cyber system in a seamless and timely manner. Time response of the authentication process is an extremely important issue.
ARPAe Project - (GT, SouCo, NYPa, EPRI)
Resilient Centralized Substation Protection and Control (rCSP)

Core Technology: Dynamic State Estimation Based Centralized Protection Scheme
Data Integrity

1. Instrumentation Channel Errors
2. Hidden Failures
3. Cyber Data Attacks
Effects of Input Data Accuracy

Quality of Data is Affected from (a) Instrumentation Channel Errors, (b) Hidden Failures and (c) cyber data attacks. All Affect Performance of protective relays (legacy relays and setting-less relays).

Relays and merging units are becoming more accurate by using higher resolution in data acquisition and higher sampling rates.

Errors from instrumentation channels remain practically the same. Instrumentation channel errors have been much higher than the errors introduced by the data acquisition even in earlier generations of sensor less systems.

Merging Units offer a unique opportunity to perform error correction within a merging unit → MU provides corrected data in primary quantities.

Error correction enables more reliable detection of cyber data attacks
Impact of Hidden Failures/Cyber Attacks

Hidden failures and cyber attacks corrupt the data “seen” by a relay, legacy or setting-less protective relay.

Hidden failures/cyber attacks will cause relay mis-operation whether it is a legacy or a setting-less protective relay.

Need to identify hidden failures/cyber attacks and avert relay mis-operations.

Present State of Art: Some legacy relaying schemes can identify some hidden failures and inhibit relay operation. No capability to take corrective action. No capability to detect data alteration by cyber-attacks.
Proposed Method for Securing Data

Supervising Substation Dynamic State Estimator

Substation Bus (Phasor Data)

Setting-Less Relay 1

Setting-Less Relay n

Process Bus

Merging Unit

Merging Unit

Merging Unit

Merging Unit

Protection Zone 1

Estimation Based Protection for Zone 1

Protection Zone n

Estimation Based Protection for Zone n

Replacement of Compromised Data with Estimated Data
Proposed Method for Securing Data

Supervising Substation Dynamic State Estimator

Extreme Redundancy

Substation Bus (Phasor Data)

Settingless Relay 1

Replacement of Compromised Data with Estimated Data

Settingless Relay n

Process Bus

Merging Unit

Protection Zone 1

Estimation Based Protection for Zone 1

Merging Unit

Protection Zone n

Estimation Based Protection for Zone n

Merging Unit
Hypothesis Testing: Observations

At substation level redundancy is high (over 2000%)
System is continuously running.
Probability of simultaneous failure events is low

Hypothesis Testing: Mechanics

Identify suspect measurements from residuals
Group suspect data with certain criteria
Determine “faulted devices” from setting-less relays output
Dynamic State Estimation Based Centralized Protection Scheme (rCSP)

Hypothesis Type 1 (H1): (determine if a hidden failure exists) Remove suspect measurements and rerun DSE. If probability high → removed measurements are bad → identify root cause → issue diagnostics → replace bad data with estimated values. End hypothesis testing. Otherwise go to H2.

Hypothesis Type 2 (H2): (determine if a fault decision is correct). For the reported faulted device, remove all internal device measurements and remove the faulted device model from the substation model. Then rerun DSE. If probability high → the device is truly experiencing an internal fault. Allow zone relay to trip the faulted device. End hypothesis testing.

Hypothesis Type 3 (H3): (simultaneous hidden failure and fault) This test combines type 1 and type 2 hypothesis testing to cover the case of a simultaneous fault and a hidden failure. If affirmative, end hypothesis testing. Otherwise go to H4.

Hypothesis Type 4 (H4): (cyber attack) Remove data originating from an IED. Then rerun DSE. If probability high → the IED has been compromised.
Examples of Intrusion
Numerical Example
Case 1: Primary Fuse Blown Y-Y, PT-4A

Sequence of Events

Time (seconds)

<table>
<thead>
<tr>
<th>Event</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

- **Fuse Blown**
- **6 MW Load Switched On**
- **6 MW Load Switched Off**

5 Protection Zones:
- 115 kV Transmission Line
- 115 kV Bus
- 115/13.8 kV, 36 MVA Transformer
- 13.8 kV Bus
- 13.8 kV Distribution Line (one of the two)
Numerical Example

Case1: Primary Fuse Blown Y-Y, PT-4A Setting-less Relay of Transformer Zone

- Transformer Zone LV Side PhA (V)
  - 22.82 kV
  - -11.60 kV
  - 11.61 kV
  - -11.63 kV
  - 11.64 kV
  - -13.29 kV

- Transformer Zone LV Side PhB (V)

- Transformer Zone LV Side PhC (V)

- Confidence Level
  - 100.0
  - 0.000

- Trip Decision
  - 1.500 s
  - 3.121 s

Highest Values of Normalized Residual

- Normalized Residual
  - 60
  - 50
  - 40
  - 30
  - 20
  - 10
  - 0

- Instrumentation Channels
  - PT-4A
  - PT-5A
  - PT-5A
  - PT-1A
  - PT-1B
  - PT-2A
  - PT-2B
  - PT-3A
  - PT-3B
  - PT-4A
  - PT-4B
  - PT-5B
  - PT-5C
  - PT-6B
  - PT-6C
  - PT-6C
  - CT-9A

Cybersecurity Lecture Series
August 23, 2019
Numerical Example

Case 1: Primary Fuse Blown Y-Y, PT-4A
Centralized Protection Scheme:

- Confidence Level
  - 200.0
  - 200.0
  - Confidence Level
  - 1.000
  - 0.000

- Hidden Failure Status
  - 1.000 u
  - -1.000 u

- Faulty Zone Status
  - 0.000 s
  - 4.992 s

- PT-4A Hidden Failure
  - 1.000 u
  - -1.000 u

- PT-4B Hidden Failure
  - 1.000 u
  - -1.000 u

- PT-4C Hidden Failure
  - 0.000 s
  - 4.992 s
Numerical Example

Case1: Primary Fuse Blown Y-Y, PT-4A
Compromised Data Correction:

- Abnormality detection
- Root cause analysis
- Estimated data streaming and replacement
- 2 cycles

Graphs showing voltage levels and trip decisions over time.
Example of Intrusion Detection

Data Attack Experiments:

- Attackers were given access to system.
- They stage their own attacks, system does not monitor their activity.
- Attack → Change Relay Settings: from 1200:5 to 2400:5
Example of Intrusion Detection

Performance Characteristics:

• Detection of data attack is almost instantaneous (25 ms or less). It is detected at the first execution of the dynamic state estimation after the attack. Dynamic state estimation executes once per 16.66 ms.

• Identification of compromised device is also fast (an additional 8 ms) by hypothesis testing. It also provides probability of certainty.

• Corrective actions: (a) quarantine compromised device, (b) block any access to the system, (c) sanitize and restore.

• Assuming that attacks can occur at one device at a time, an attack can be foiled and stopped in real time.
Context Based Command Authentication

• Capture command,

• Determine effect of command on system using real time model and faster than real time simulation and

• Authenticate/Block command on the basis of the effects on the system.
Example of Intrusion Detection

**Attack Experiments:** Attackers were given access to system. They stage their own attacks, system does not monitor their activity.

**Attack:** at time $t = 2.5$ sec, a malicious control is sent to open the breaker of the Eastgate-Scenic Hills line in the Eastgate substation.
Numerical Example of GPS Spoofing Detection

Without GPS Spoofing

With GPS Spoofing
SouthernCo - Georgia Tech Work
Implementation of DSE on Three SoCo Substations

Additional Benefits
- Reduced Control House Size
- Reduced Wiring
GT Laboratory (PSCAL)
Dedicated Lab for Protection, Control & Cyber Security Testing: Continuous Operation of Fully Automated Substation: Complete Substation Cyber Infrastructure

Configuration is a full replica of the IT infrastructure of a modern substation with multi-vendor equipment.

Combines numerical relay architecture with new architectures based on merging units.

It is driven by a high fidelity simulator capable of reproducing real life conditions.

Unique capability for simultaneous testing of protection, control and cyber security.

Enables realistic testing of Intrusion Detection System in an almost field conditions environment using the PB-PCcoM approach.

Additional Cyber Security
Encrypted Hash generated by MU and embedded in streaming data.
Concluding Remarks

The industry supported by IEEE and CIGRE Efforts Move Towards the DIGITAL SUBSTATION.

The entire process is becoming fully automated (many efforts towards autonomy) with self healing capabilities against data errors, hidden failures and cyber attacks.

The technologies under development offer three distinct benefits:

(a) Drastically improved operational reliability
(b) Reliable defenses against cyber attacks
(c) Reduced Cost
Τέλος