An Approach To Improving The Physical And Cyber Security Of A Bulk Power System With FACTS

Mariesa Crow & Bruce McMillin
School of Materials, Energy & Earth Resources
Department of Computer Science
University of Missouri-Rolla

Stan Atcitty
Power Sources Development Department
Sandia National Laboratories
ACKNOWLEDGMENTS

- Funded in part by the Energy Storage Systems Program of the U.S. Department Of Energy (DOE/ESS) through Sandia National Laboratories (SNL).
Problem Motivation

- Prevent Cascading failures:
  - 2003 Blackout

- Causes
  - Physical & Cyber contingencies
  - Deliberate disruption
    - Hackers
    - Terrorist Activity
Proposed Solution

Flexible AC Transmission Systems (FACTS)
- Power Electronic Controllers
- Means to modify the power flow through a particular transmission corridor
- Integration with energy storage systems
US FACTS Installations

- **AEP/ Unified Power Flow Controller /100 MVA/ EPRI**
- **NYPA/ Convertible Static Compensator/ 200 MVA**
- **Vermont Electric/ STATCOM/ 130 MVA/ Mitsubishi**
- **Northeast Utilities/ STATCOM/ 150 MVA/ Areva (Alstom)**
- **TVA STATCOM/ 100MVA EPRI**
- **San Diego G&E/ STATCOM/100 MVA Mitsubishi**
- **Eagle Pass (Texas) Back-to-back HVDC 37 MVA/ ABB**
- **CSWS (Texas) STATCOM/ 150 MVA / W-Siemens**
- **Austin Energy STATCOM/ 100MVA ABB**
Decentralized Infrastructures

- Communication and coordination
  - Scheduling - Distributed Long-Term control
  - Interaction – Local Dynamic control
- Vulnerabilities of the combined physical/ cyber system
- Recovery and protection from physical faults and/or cyber attacks and/or human error
Identify cascading failure scenarios for test systems
FACTS Placement and Control
FACTS Control

- Distributed Long-Term control algorithms for FACTS settings
  - Run by each processor in each FACTS
- Alternatives
  - Max-flow algorithms
  - Local optimizations
  - Agent-based framework
- Assessment
  - Reduction of Overloads
  - Computability
FACTS Placement

- Placement
  - Place few FACTS in a large network for maximum benefit

Evolutionary Algorithms (EAs) will be used to place FACTS devices in the network
Performance Index Metric

\[
PI = \sum_{\text{Contingency}} P_{\text{Contingency}} \left( \sum_{\text{line}} \omega_{\text{line}} \left( \frac{S_{\text{line}}}{S_{\text{max}}^n} \right)^2 \right)^k
\]
FACTS Interaction Laboratory (FIL)
FIL Overview

- Construct a Laboratory System to Study and Mitigate
  - Cascading Failures
  - Deleterious effects of interacting power control devices
  - Cyber Vulnerabilities
- Hardware in the Loop (HIL)
  - Real-time Simulation Engine
    - Simulate Existing Power Systems
    - Inject Simulated Faults
  - Interconnected laboratory-scale UPFC FACTS Device
    - Measure actual device interaction
HIL Laboratory Interface

Power System Simulation Engine

Machine 1
FACTS1
Controllable Load

Machine 2
FACTS2
Controllable Load

Machine 3
FACTS3
Controllable Load

D/A output
A/D input
D/A output
A/D input
D/A output
A/D input
FACTS – Flexible AC Transmission System Prototype Device
FACTS Interaction Laboratory

UPFC

Simulation Engine

HIL Line
Cyber Fault Detection
Fault Tolerance

- Define correct operation of the power system with FACTS/ESS
- Embed as executable constraints into each FACTS/ESS computer
- FACTS/ESS check each other during operation of distributed control algorithms
Cyber Fault Injection

- Attempt to confuse the FACTS embedded computers
- Attempt to disrupt the communication between FACTS embedded computers
- Confuse the power system’s operation
## Error Coverage of Distributed Executable Correctness Constraints (Maximum Flow Algorithm)

<table>
<thead>
<tr>
<th>Error Type</th>
<th>Errors Detected By</th>
<th>Unreported Errors</th>
<th>Coverage of Errors Detection</th>
<th>Average Time (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Program</td>
<td>Timeout</td>
<td>Connection Termination</td>
<td></td>
</tr>
<tr>
<td>Edge Error (over all edges)</td>
<td>117 (100%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>Vertex Error (over all vertices)</td>
<td>115 (98.3%)</td>
<td>0 (0%)</td>
<td>2 (1.7%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>Lose All</td>
<td>0 (0%)</td>
<td>100 (100%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>Flow Messages</td>
<td>0 (0%)</td>
<td>131 (97.0%)</td>
<td>0 (0%)</td>
<td>4 (3.0%)</td>
</tr>
<tr>
<td>Randomly Lose All Flow Messages</td>
<td>50 (100%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>Alter All</td>
<td>50 (100%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>Randomly Alter All Flow Messages</td>
<td>100 (100%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>Invert All Accept/Reject Messages</td>
<td>50 (100%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
<td>0 (0%)</td>
</tr>
</tbody>
</table>
System Dynamic Control
A decentralized power network embedded with FACTS devices can be viewed as a hybrid dynamical system (Differential-algebraic-discrete-event).

While the FACTS devices offer improved controllability, their actions in a decentralized power network can cause deleterious interactions among them.
Performance of FACTS controllers with ideal observability

Uncontrollable modes in generator speeds due to device interactions
Project Benchmarks

- Construction of HIL
- Demonstration of Cascading Failures
- Placement and Control
- Hardware/Software Architecture
- Cyber Fault Detection
- Dynamic Control
- Visualization
Special Thanks

- Imre Gyuk – DOE Energy Storage
- Stan Atcitty – Sandia National Lab
- John Boyes – Sandia National Lab