A Simulation Testbed for Cascade Analysis

_Saqib Hasan_¹, Abhishek Dubey¹, Ajay Chhokra¹, Nagabhushan Mahadevan¹, Gabor Karsai¹, Rishabh Jain², Srdjan Lukic²

¹ Vanderbilt University
² North Carolina State University
Cascading Failures: Power Transmission Systems

- Power systems are vulnerable to both physical Faults and cyber Faults.
- Cyber Faults in protection assembly can lead to severe cascading failures.
- **Dec 2015 Ukraine** and **Aug 2003 USA** are recent blackout cases.
- Diagnosing and predicting cascading failures effectively requires the consideration of behavioral models of these protection assembly.
- Behavioral models can introduce cyber-faults and produce new cascading trajectories.
Contributions

• Detailed behavioral models of protection Assembly are developed.
  – **Nominal** and **faulty modes** of operation.
  – For simulation based evaluation **Cyber-Faults** introduction at **specific time**.
  – **Ordering** of events are taken into account.

• A contingency analysis framework is proposed.
  – To study the **evolution of cascades** in the **presence of cyber-faults**.
  – Analysis provides **new cascade evolution trajectories** not obvious otherwise.
  – Case study performed on **IEEE-14 Bus System**.
Protection Assembly and Cyber-Faults

• Protection Assembly
  – **Distance Relay** Behavioral Model.
  – **Over-Current Relay** Behavioral Model.
  – **Circuit Breaker** Behavioral Model.

• Cyber-Faults
  – **Missed Detection Faults**: Relay fails to detect the anomaly.
  – **Spurious Detection Faults**: Relay incorrectly detects the anomaly.
  – **Stuck breaker Faults**: Breaker does not operate as commanded.
Distance Relay Behavioral Model

- **Primary protection** in electrical power systems.
- Three zone reaches (Zone1, Zone2 and Zone3).
- Normal mode operation and operation under cyber-faults.

[Diagram of Distance Relay Behavioral Model]
Over-Current Relay Behavioral Model

- Used as a **back-up protection** in electrical power systems.
- Normal mode operation and operation under cyber-faults.
Circuit Breaker Behavioral Model

- **Physically connects or disconnects** the components in electrical power systems.
- Normal mode operation and operation under cyber-faults.
Towards Contingency Analysis

- **Identify critical sets** causing cascading failures leading to blackouts.
- **Integration of protection assembly** behavioral models.
- **Captures time between events** and **trigger cyber-faults** at specific instants.
- **Arbitrary cyber-faults** can be introduced at **any time instant** during the simulation.

![Contingency Analysis Diagram](image)
System Under Test

- IEEE-14 bus system is used for analysis.
- Each transmission line is protected by a pair of protection assembly.
Analysis Results

• How cyber-faults leads to severe cascading failures causing blackouts?
• How the proposed framework can be used for identifying new blackout causing contingencies?
• Case 1
  – Physical fault in transmission line ‘L3_4’ at t= 0.5 sec.
  – No cascading failure.
• Case 2
  – Physical fault in transmission line ‘L3_4’ at t= 0.5 sec.
  – Cyber-fault in circuit breaker ‘PA_BR4’ at t= 0.5 sec.
  – Cyber-fault in distance relay ‘PA_DR27’ at t= 2.0 sec.
  – Cascading failure resulting in blackout.
### Analysis Results - Sequence of Cascading Events

<table>
<thead>
<tr>
<th>Time (sec)</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.500</td>
<td>F: 3φ-G fault - Line L3-4, Stuck close fault - PA_BR4.</td>
</tr>
<tr>
<td>0.501</td>
<td>D: Z1, Z3 in PA_DR[3,4], PA_DR1, 'P1_OL' in PA_OR3, 'P2_OL' in PA_OR[9,5,13], 'P3_OL' in PA_OR[9,5,21]. CR: 'cmd_open' in PA_BR3.</td>
</tr>
<tr>
<td>0.532</td>
<td>S: st_open-PA_BR3 is opened. L: Line L3_4 tripped partially.</td>
</tr>
<tr>
<td>2.000</td>
<td>F: Spurious detection fault in PA_DR27. CS/CR: 'cmd_open' in PA_DR27/PA_BR27.</td>
</tr>
<tr>
<td>2.031</td>
<td>S: 'st_open' - PA_BR27 is opened. L: Line L6_12 is removed.</td>
</tr>
<tr>
<td>5.536</td>
<td>D: 'P1_OL' in PA_OR[25,33], 'P2_OL' in PA_OR{35,40}, 'P3_OL' in PA_OR{29,37}. S: 'st_open' - PA_BR13 is opened. L: Line L5_4 is disconnected.</td>
</tr>
<tr>
<td>6.536</td>
<td>D: 'P1_OL' in PA_OR31.</td>
</tr>
<tr>
<td>7.503</td>
<td>CS/CR: 'cmd_open' in PA_OR15/PA_BR15.</td>
</tr>
<tr>
<td>7.534</td>
<td>S: 'st_open' - PA_BR15 is opened. L: Line L7_8 is removed.</td>
</tr>
<tr>
<td>7.538</td>
<td>CS/CR: 'cmd_open' in PA_OR[25,33]/PA_BR[25,33].</td>
</tr>
<tr>
<td>14.602</td>
<td>S: 'st_open' - PA_BR1 is opened. L: Line L2_3 is tripped.</td>
</tr>
</tbody>
</table>

**F**: Occurrence of fault events, **D**: Detection of zone faults and overloads, **CS/CR**: Send/Receive commands from relays to circuit breakers, **S**: Status of the circuit breakers, **L**: Outage of lines.
Conclusion and Future Work

- Detailed behavioral models of protection assembly are presented.
- Capability to introduce cyber-faults at specific instants.
- A contingency analysis framework is proposed.
- Case study is presented to identify severe cascading causing contingencies resulting in blackout.
- As part of the future work, we will look at the scalability of the approach.
Acknowledgements

- National Science Foundation (NSF).
THANK YOU!
Analysis Results- Sequence of Cascading Events Waveforms