PUTTING A NUMBER TO GRID RESILIENCY

- Quantifying Cyber-physical System Resilience!
  - Create a metric that integrates factors from cyber and physical domains and integrate them to one, easy-to-understand metric
  - Use system level and device level factors, graph-theory-based system analysis, physics-based analysis, and system real-time measurements
- Resulting metric enables the operator to “Anticipate” any event/attack, prepare to “Withstand” that, and provide proactive suggestions for faster “Recovery”

KEY CHALLENGE

- For device-level, a data-driven resilience metric and countermeasure against ongoing attacks that evade software-based detection
  - Analysis of the controller software to measure their intrusion resilience
  - Analysis of physical dynamics to understand their temporal evolution

WHAT WE DO

Distribution System Resiliency: Cyber-Physical Resiliency (CyPhyR)

- Enables measuring resiliency using data from cyber and physical systems.
- Suggests control decisions for resilient planning and operation of the microgrid.
- Resiliency is formulated based on graph theory-based indices and cyber-power system characteristics.

RESULTS

- IEEE 13 node test feeder is connected on bus 12 of 39-bus transmission system.

<table>
<thead>
<tr>
<th>Cases</th>
<th>LoI</th>
<th>SPDI</th>
<th>MWAi</th>
<th>MVA/</th>
<th>Physical-resilience score</th>
<th>Cyber-resilience score</th>
<th>TRAM score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 1</td>
<td>1</td>
<td>30.3517</td>
<td>0.3708</td>
<td>5.9694</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Case 2</td>
<td>1</td>
<td>19.0514</td>
<td>0.3703</td>
<td>5.9239</td>
<td>0.9177</td>
<td>1</td>
<td>0.9588</td>
</tr>
<tr>
<td>Case 3</td>
<td>1</td>
<td>7.4183</td>
<td>0.3688</td>
<td>5.8022</td>
<td>0.8322</td>
<td>1</td>
<td>0.9161</td>
</tr>
<tr>
<td>Case 4</td>
<td>1</td>
<td>25.9725</td>
<td>0.2341</td>
<td>5.1913</td>
<td>0.9299</td>
<td>0.98</td>
<td>0.9587</td>
</tr>
</tbody>
</table>

Transmission resiliency at bus 12

- In case of generator loss at bus 32 in transmission system effects distribution system resiliency.

HOW DO THE NUMBERS HELP?

- CyPhyR and TRAM help operators monitoring the real-time grid resiliency
- Reflects the resiliency of the system during different stages of a cyber-attack, including
  - vulnerabilities detected and exploited,
  - elevated privileges gained,
  - malicious physical control actions such as reconfiguration of the microgrid
- Potential attacks on control devices are interrupted in real-time

INTERACTION WITH OTHER PROJECTS

- We’re interested in collaboration with industry and vendors to get feedback on our models, techniques, and tools to determine the real-time resiliency of a system.
- We anticipate collaboration with ongoing CREDC activities on intrusion detection and runtime security monitoring, which will be used to update resilience measurements based on the current state of the system.

FUTURE EFFORTS

- Specific applications requirements of smart grid depend largely on the communication network of the grid. In future, we will try to derive metric defining network configuration level complexity issues of smart grid and incorporate these into our tools to enhance resiliency through analyzing the network configuration.
- We will deploy and validate our metric on real-world scenarios.
- Implementing operational controls or system restoration procedures from control center.
- We are currently working on the details of our preliminary intrusion resilience metric design and system-level resiliency metric.

REFERENCES