Metrics and Tools for Measuring Cyber Resiliency of Electric Grids

V. Venkataramanan, Tushar, V. V. G. Krishnan, A. Srivastava, A. Hahn – Washington State University
A. Ding and S. Zonouz - Rutgers University

PUTTING A NUMBER TO RESILIENCY

- *Make cyber-physical resilience measurable!*
  - 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 measurements
  - Resulting metric enables *better planning/ decision support* and *better visibility* for operator!

KEY CHALLENGE -

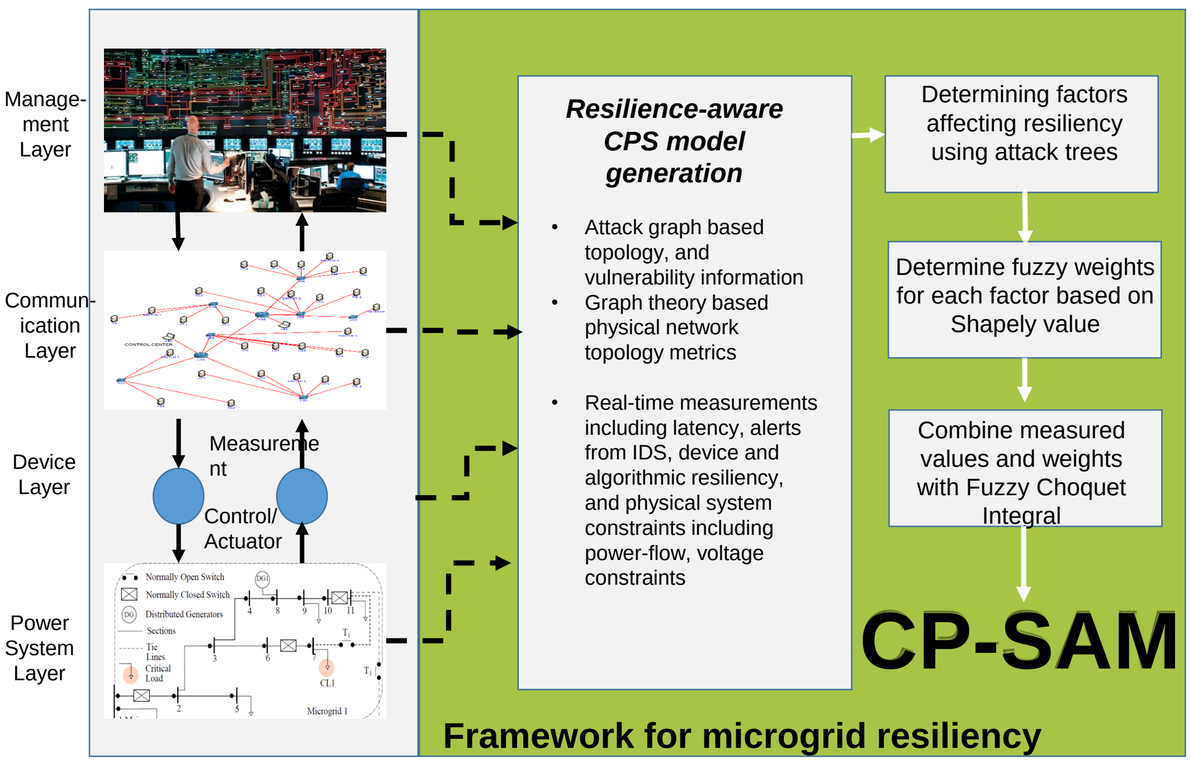
Considering various factors from *different domains* and *integrating* them to compute a resilience metric

- 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

System Level Metrics: CP-SAM

- Security assessment and resiliency – system security with contingencies will enable resiliency
- What are the factors that affect the resiliency of the electric grid, and how to measure this resiliency?
- CP-SAM is a comprehensive metric that combines cyber and physical factors into a single metric instead of studying the effect of cyber vulnerabilities on the power system

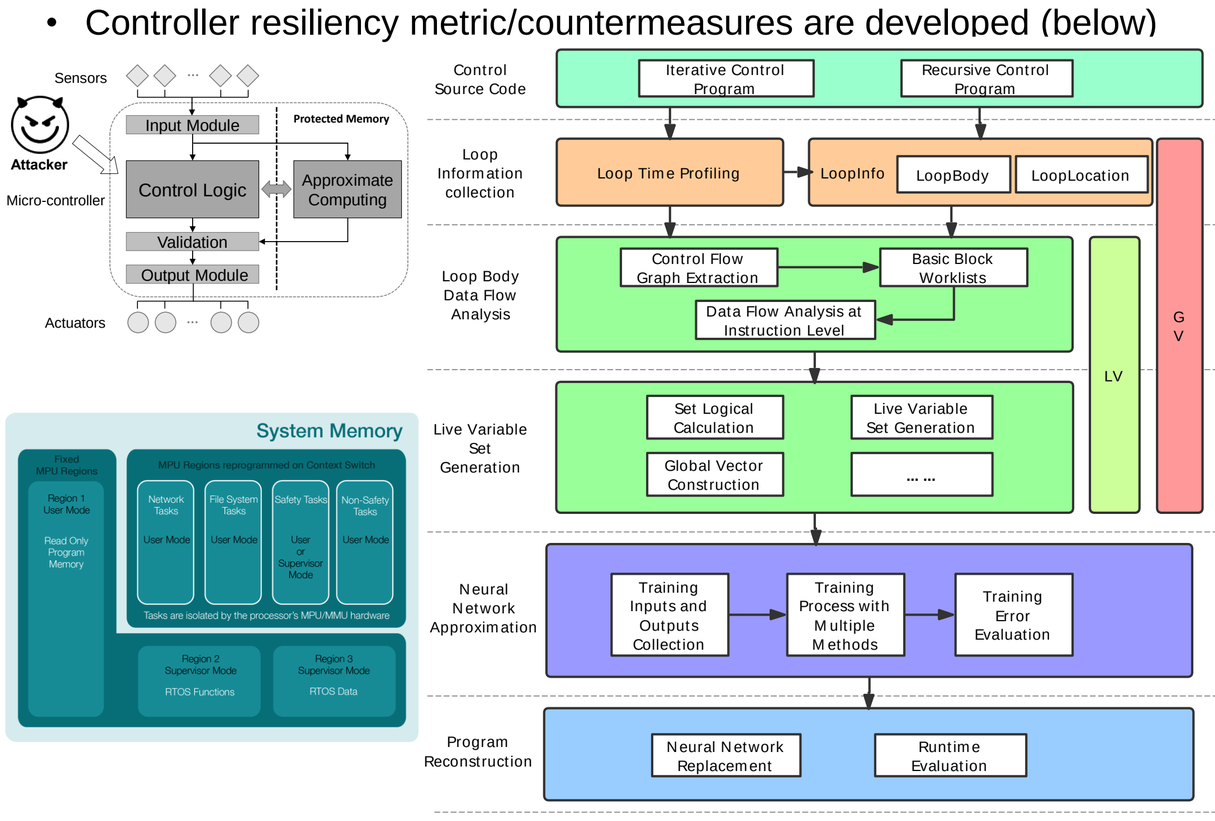


Framework for microgrid resiliency

- Transmission system resiliency metric is computed at each transmission system substation that is aggregated with distribution and microgrid resiliency to obtain the overall system resiliency
- Attributes defining transmission resiliency are:
  - Network configuration
  - Redundancy in network and source of power supply
  - Vulnerabilities like a single transmission line in all redundant paths
  - Variability and Availability of power supply

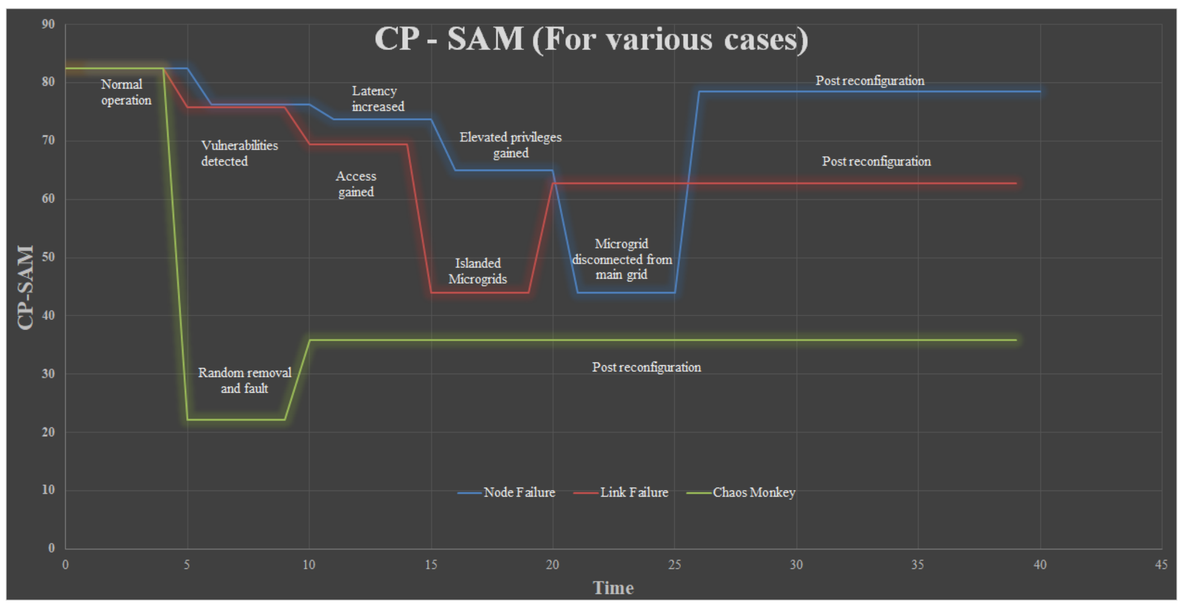
Device Level Resiliency

- Controller resiliency metric/countermeasures are developed (below)

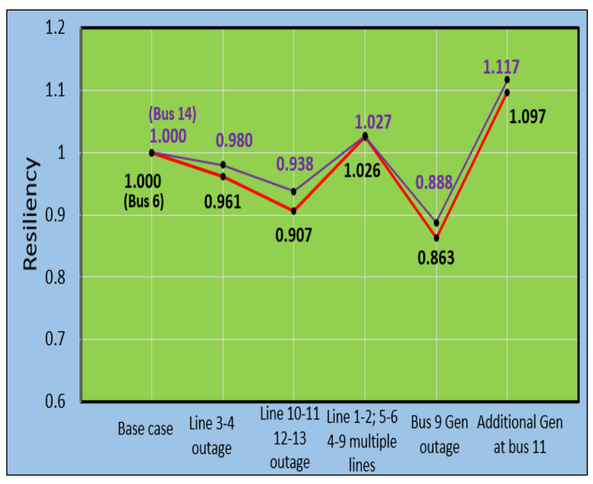


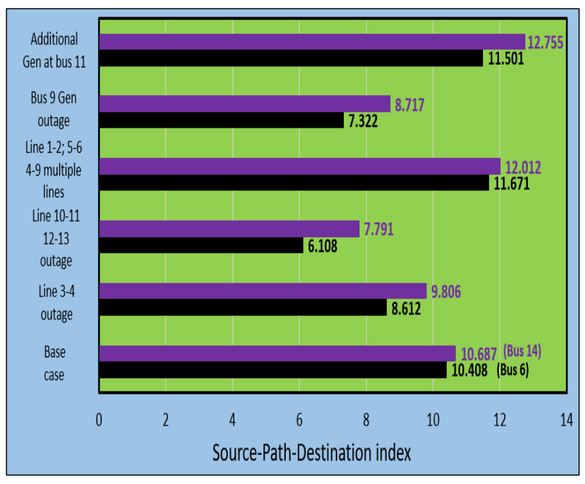
RESULTS

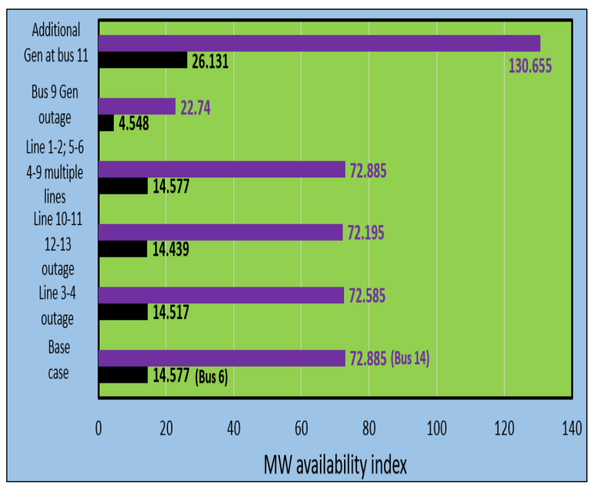
- Three scenarios are presented – i) Loss of node, ii) Loss of link, iii) Netflix Chaos Monkey inspired random failure
  - CP-SAM updates over time to help operator quickly understand the resilience of the system

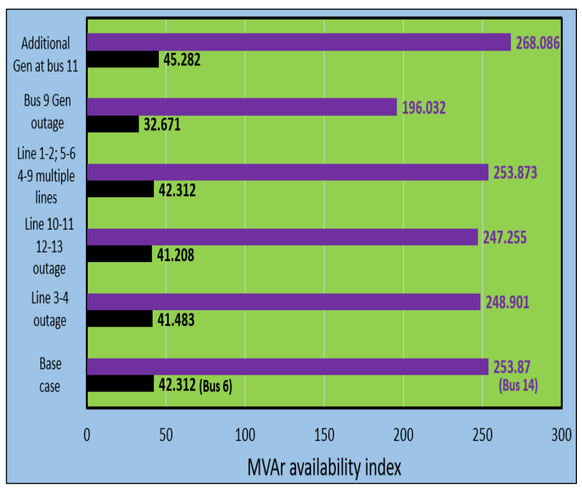


CP-SAM for various cases









Transmission physical resiliency for various cases

HOW DOES THIS NUMBER HELP?

- CP-SAM can be use by operators to monitor the real-time resiliency of the system
- CP-SAM reflects the resilience of the system for various stages of a cyber-attack including vulnerabilities detected and exploited, elevated privileges gained, malicious activity resulting in physical impact, and effect of control actions such as reconfiguration of the microgrid
- Controller device attacks are terminated and responded to 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

- Working on the details of our preliminary intrusion resilience metric design and system-level resilience metric.
- Will deploy and validate our metric on real-world testbeds.
- Will develop device-level intrusion response capabilities and system-level defense mechanisms to enhance resiliency.

https://cred-c.org/researchactivity/metrics-and-tools-measuring-cyber-resiliency-electric-grids

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY