Resiliency Metrics for Electric Grid and Analyzing Impact of Defense Mechanisms

Cyber-Physical Resiliency Metric for Microgrids

V. Venkataramanan, A. Ding, A. Hahn, A. Srivastava, S. Zonouz, and C. Hauser

GOALS

- Modeling and simulation of cyber-physical systems to analyze the impact of cyber events on the power grid.
- Develop system-level quantitative cyber-physical resilience metrics.
- Perform device-level firmware analysis, security monitoring, and adaptation for quantitative resilience assessment and improvement.
- Explore tradeoffs offered by various defense mechanisms to enhance resiliency.

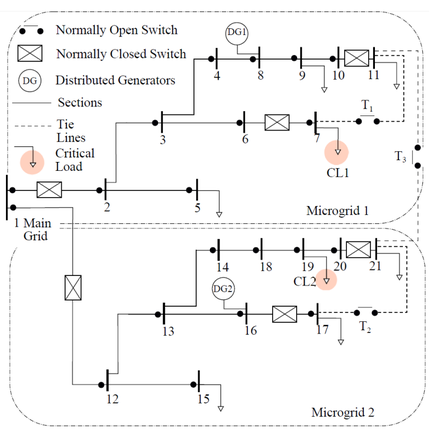
FUNDAMENTAL QUESTIONS/CHALLENGES

- Design representative cyber-physical test cases for the grid (microgrids and transmission systems in different phases) and realistic attack modeling with hardware-in-the-loop testbeds using RTDS, OPAL-RT, and other testbed components.
- Develop cyber-physical resiliency metrics that can be calculated automatically to quantify the power grid resilience against the realistic attack models.
- Static analysis of device firmware executables for architecture/format and design of distributed security measures on embedded devices.
- Automated adaptation of the system architecture to improve its overall resilience based on the defined metrics and the previously explored defenses to evaluate their effectiveness.
- Determine the domain-specific features for EDS that could be leveraged for firmware-level intrusion detection, such as live memory monitoring for power plant safety parameter value ranges.

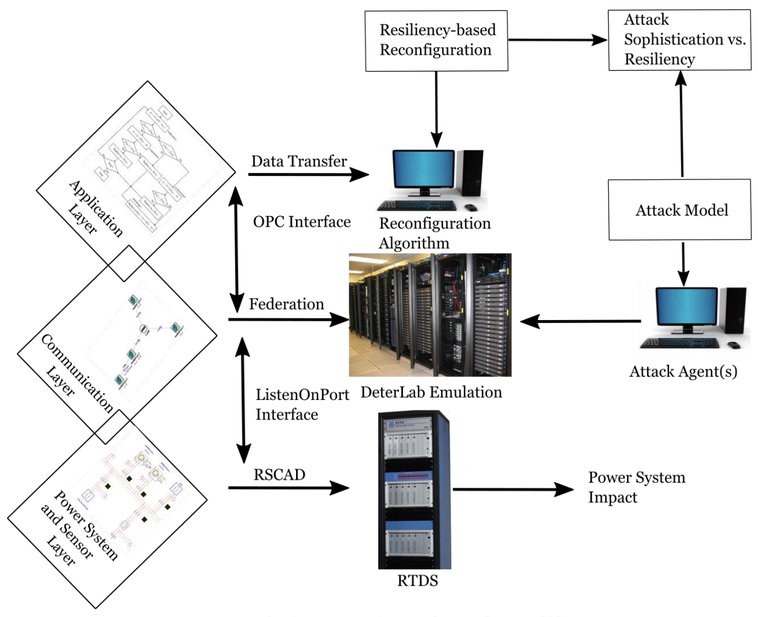
RESEARCH PLAN

- The proposed approach will focus on the modeling and real-time simulation of various cyber attacks and then on analyzing their impact on the physical power grid, focused on networked microgrids and transmission systems.
- The proposed metrics will attempt to extend and combine common impact metrics from both the cyber domain (e.g., CVSS, CWSS) and the power domain (e.g., topological and system resiliency).

Device-level security for resiliency metric



Two proximal CERTS microgrids test system

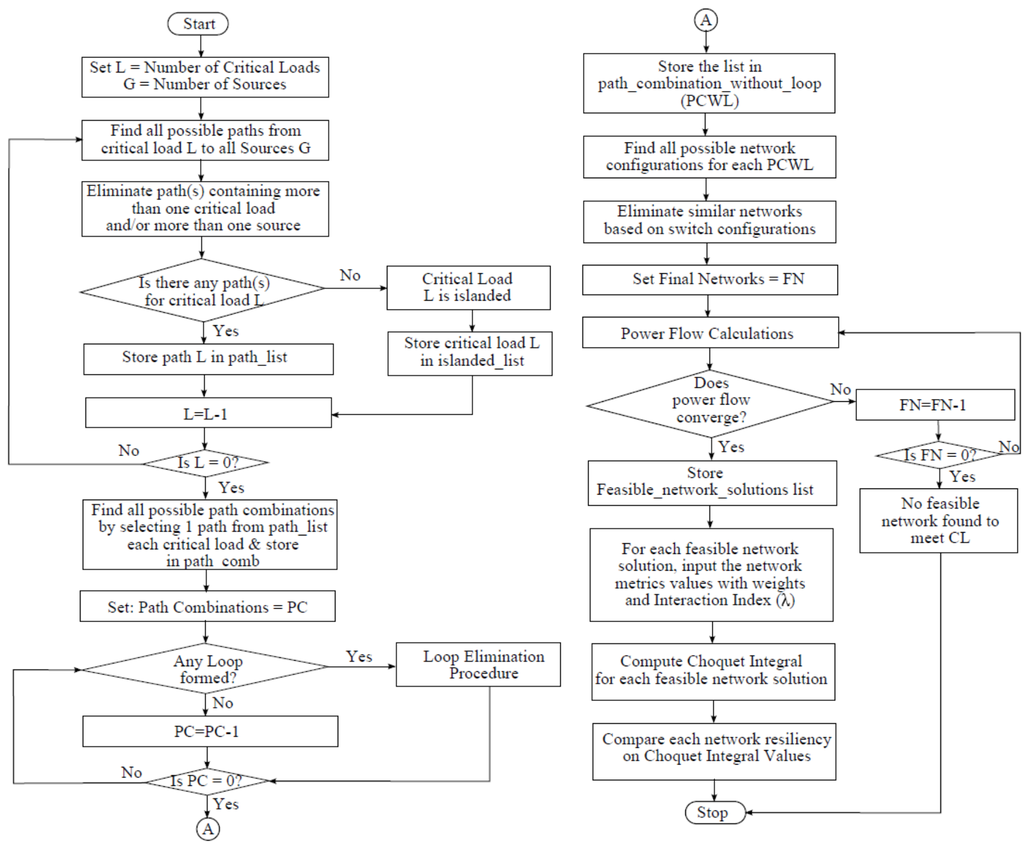


Framework for system-level resiliency

- Analyze trade-offs offered by cyber-defense mechanisms and physical system strengthening mechanisms to enable resiliency, by exploring methods such as reconfiguration, redundancy, partitioning, non-persistence, and automated response.
- Analyze vulnerabilities, attacks, and defense mechanisms to study their impact on grid resiliency using hardware-in-the-loop CREDC test-beds.
- Analyze the security impact of local and distributed device-level intrusions on low-level firmware and embedded control logic through online reference monitors and runtime quantitative resilience metrics assessment.

RESEARCH RESULTS

- A preliminary power system resilience metric that can quantify the resilience of all possible system configurations.
- A device-level security metric regarding how likely it is that the device firmware and software stack will accomplish its functional objectives.
- A preliminary design of a cyber-physical resilience metric based on numerous properties of cyber and physical system components.
- A study on the impact of cyber attacks on the microgrid's resiliency, and how it varies because of attack sophistication.

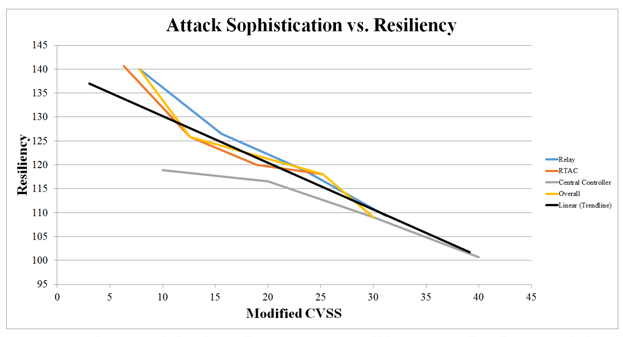


Reconfiguration Algorithm based on Resiliency

FINAL NETWORKS WITH CORRESPONDING SIMILAR POSSIBLE NETWORKS AND SWITCH CONFIGURATIONS

Final networks	Similar Possible Networks	Sectionalizing Switches (NC) 2-1	12-1	7-1	11-10	16-17	20-21	Tie-line Switches (NO) 11-7	21-11	21-17
N^1	N_1, N_4, N_9, N_{12}	C	C	C	C	C	C	O	O	O
N^2	N_2, N_{10}	C	O	C	C	C	C	O	C	O
N^3	N_3, N_{11}	O	C	C	C	C	C	O	C	O
N^4	N_5, N_8	C	C	O	C	C	C	C	O	
N^5	N_6	C	O	O	C	C	C	C	C	O
N^6	N_7	O	C	O	C	C	C	C	C	O
N^7	N_{13}, N_{16}, N_{18}	C	O	O	C	C	O	C	C	C
N^8	N_{14}, N_{17}, N_{19}	O	C	O	C	C	O	C	C	C
N^9	N_{15}	O	O	O	C	C	O	C	C	C

Reconfiguration Algorithm Result



Attack Sophistication vs. Resiliency of Microgrid

BROADER IMPACT

- The developed metric will enable an operator to choose between alternative network configurations and defenses to maximize resiliency.
- The research will facilitate the deployment of the intrusion response and recovery engines within the cyber-physical infrastructures.
- The metric will enable operators to obtain the resiliency of their systems in real time and make intelligent decisions to protect/improve the resiliency of their system.

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

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

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