Metrics and Tools for Measuring Cyber-Physical Resiliency of Electric Grids

Partha Sarker, K. S. Sajan, Zhijie Nie, Anurag K. Srivastava, Adam Hahn

Washington State University

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

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

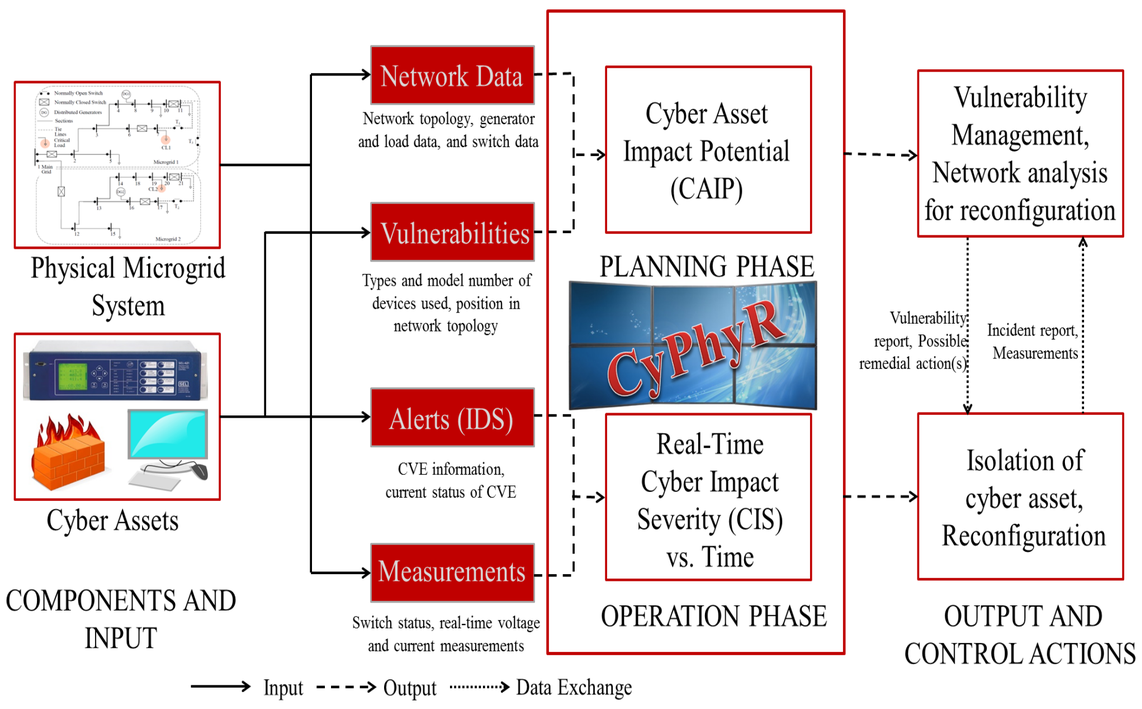
➢ Dependency of one system on another system in terms of resiliency

- 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)

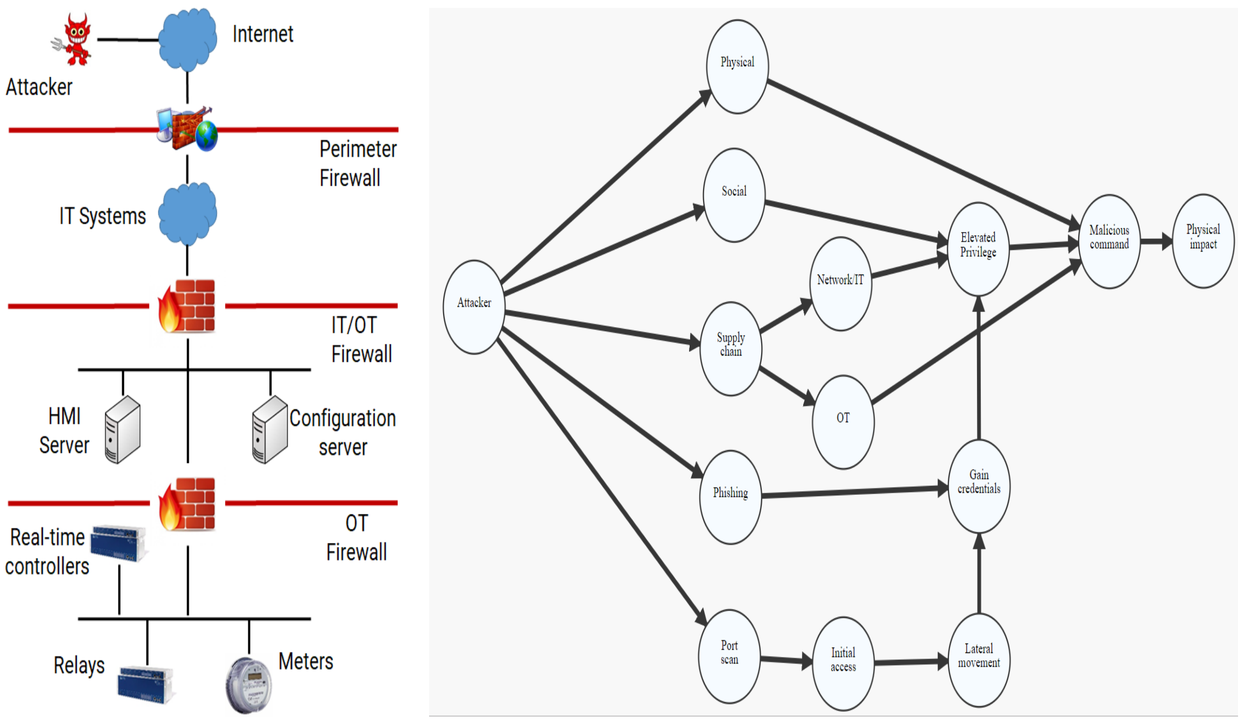
- Enables measuring resiliency using data from cyber and physical systems.
- Suggests control decisions for resilient planning and operation of the microgrid.
- Resiliency is formulated based on graph theory-based indices and cyber-power system characteristics.



Framework for distribution system resiliency

Transmission System Resiliency Assessment Metric(TRAM)

- Transmission system resiliency metric is computed at each transmission system substation.
- Physical resiliency considers:
  - Network configuration
  - Redundancy in network and sources of power supply
  - Vulnerabilities like a single transmission line in all redundant paths
  - Availability and variability of power supply
- Cyber resiliency score considers detailed substation cyber model, based on the defense-in-depth (DID) model and attack graph.



Defense-in-depth and attack graph models

RESULTS

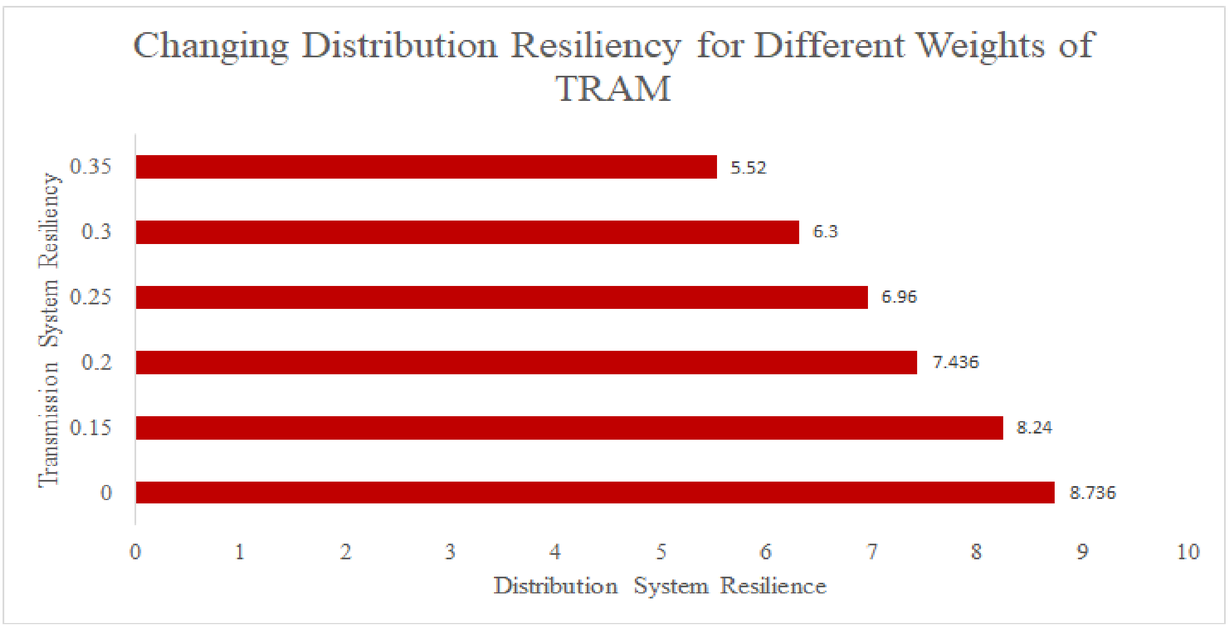
- IEEE 13 node test feeder is connected on bus 12 of 39-bus transmission system.

Cases	LoLI	SPDI	MWAI	MVArAI	Physical-resilience score	Cyber-resilience score	TRAM
Case 1	1	30.3517	0.3708	5.9694	1	1	1
Case 2	1	19.0514	0.3703	5.9239	0.9177	1	0.9588
Case 3	1	7.4183	0.3688	5.8022	0.8322	1	0.9161
Case 4	1	25.9725	0.2341	5.1913	0.9299	0.98	0.9587

Transmission resiliency at bus 12

Dependency of distribution system on transmission system

- 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 resilience
- Reflects the resilience 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 resilience metric.

REFERENCES

1. V. Venkataramanan, A. Hahn and A. Srivastava, "CyPhyR: a cyber-physical analysis tool for measuring and enabling resiliency in microgrids," in IET Cyber-Physical Systems: Theory & Applications, vol. 4, no. 4, pp. 313-321, 12 2019.
2. Tushar, "Measuring and Enabling Cyber-Physical Resiliency of ElectricTransmission Systems," Ph.D. dissertation, Washington State University,Pullman, WA, 2018.
3. V. Venkataramanan, P. S. Sarker, K. S. Sajan, A. Srivastava and A. Hahn, "A Real-Time Transmission-Distribution Testbed for Resiliency Analysis," 2019 IEEE Industry Applications Society Annual Meeting, Baltimore, MD, USA, 2019, pp. 1-7.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

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