CREDC
CYBER RESILIENT ENERGY
DELIVERY CONSORTIUM

Research Activity
Fact Sheet

Metrics and Tools for Measuring Cyber Resiliency of Electric Grids

Website: http://cred-c.org/researchactivity/metrics

Researchers (WSU, Rutgers): Anurag Srivastava, Adam Hahn, Saman Zonouz (Rutgers), Venkatesh Venkataramanan, Aolin Ding (Rutgers), Tushar, Vignesh Krishnan

Industry Collaboration:

- Siemens
- Currently seeking additional collaborators from industry, power utilities, and national labs.

Description of research activity: The approach used in this activity focuses on the identification and validation of metrics and tools for cyber resilience to directed attacks on power grid systems, with particular attention paid to networked transmission systems. This work takes a multi-step approach for developing resiliency metric, first for microgrid, then distribution system and finally for transmission systems. Additionally, we are developing metrics at the device level (e.g., programmable logic controllers) to measure the level of security (in terms of the infrastructural safety) a given controller code provides. The effort relies on testbed-based analysis using RTDS, OPAL-RT, communication emulators, hardware intelligent electronic devices, amplifiers, and hardware controllers to model time-critical power grid applications which will be most impacted by cyber attacks. In developing the metrics, we will extend and combine common impact metrics from both the cyber-domain (e.g., common vulnerability scoring system (CVSS), Common Weakness Scoring System (CWSS)) and the power-domain (e.g., topological and system resiliency). In addition, we will develop new metrics for devices not yet covered by standards (e.g., PLCs). We will develop tools that measure the metrics and analyze cyber resiliency, and use these tools to quantify the improvements in security that are brought about by techniques such as reconfiguration, redundancy, partitioning, non-persistence and automated response. Cyber-vulnerabilities, cyber attacks and cyber-defense mechanisms and their impact on power grid resiliency will be studied using the hardware-in-the-loop capability of CREDC testbeds.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
This research activity addresses one of the top priorities: metrics to measure security to assess and monitor risks as identified by participants at the September 2009 Roadmap Update Workshop and available as exhibit 4.3.1 of the Roadmap. Additionally, the need for testbed validation of the developed tools for resilience testing and assessment is identified in exhibit 4.4.1, which will be one of the research activities to support the developed resiliency assessment metrics tools.

Summary of EDS gap analysis: The power grid currently lacks metrics, tools or technology for quantifying operation technologies (OT) with respect to cyber resiliency to attack. These must be developed and integrated into the grid's design and operational processes to enable resilient transmission, distribution and microgrid systems. While previous work has explored both resilience in cyber systems and in the physical grid, there remains a need to develop cyber-physical metrics. Research is needed to provide a cyber-physical system model, alternative attack models, alternative metrics to analyze the impact on resiliency of the system, and tools that use those metrics to aid in the design of OT systems, as well as identify security problems after the system is installed and is running.

Full EDS gap analysis: Developing key metrics to compare system security with and without deploying defense mechanisms has been identified as the top priority for assessing and monitoring risk and increasing the resiliency of energy delivery systems [1]. Resiliency of EDS relies on being able to prepare for and adapt to changing conditions, and the ability to withstand and recover from adverse cyber-events. To measure resiliency specific to the electric grid, metrics are required to analyze the various cyber vulnerabilities and weaknesses and assess their impact on the electric grid [2-3]. Resiliency needs to be addressed at the device level as well as at the system level and should cover components from generation, transmission, distribution, microgrids, end-users and associated cyber infrastructure [4].

Tools are needed to measure resiliency and providing operational and planning support. Planning tools can be used to compare resiliency of the system with different defense mechanisms and operational tools can be used to provide decision support to operators with changing system resiliency. In addition to developing these tools, we will validate these tools on cyber-physical testbeds. This work will explore the proposed resilience metrics in multiple scenarios against a variety of attacks and defensive methods [1]. Our previous work demonstrated a usable metric for power grid physical resiliency limited to the distribution system [5] but without considering the associated cyber system. Thus there is a need to develop a metric for cyber-physical resiliency as well as to develop tools to evaluate systems according to this metric.

Bibliography:

[1]. Energy Sector Control System Working Group, “Roadmap to achieve Energy Delivery Systems Cybersecurity”, Septemeber 2011

[2]. K. Eshghi, B. Johnson, and C. G. Rieger. "Metrics required for power system resilient operations and protection." In *Resilience Week (RWS),* pp. 200-203. IEEE, 2016.

[3]. D. Nicol, "Risk Assessment of Cyber Access to Physical Infrastructure in Cyber-Physical Systems." In *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security*, pp. 1-2. ACM, 2016.

[4] Cyber Security Working Group, “Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security”, The Smart Grid Interoperability Panel, September 2010.

[5] S. Chanda, A. Srivastava. "Defining and enabling resiliency of electric distribution systems with multiple microgrids." *IEEE Transactions on Smart Grid* , no. 6, 2016, pp. 2859-2868.