CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

**Research Activity Fact Sheet**

# Real-time Situational Awareness of Risk to EDS To Cyber Attack

**Website:** http://cred-c.org/researchactivity/rtsarisk

**Researchers (OSU):** Rakesh Bobba, Eduardo Cotilla-Sanchez, Chen Huo, Arezoo Rajabi

**Industry Collaboration:**

- Currently seeking industry collaborators. Please contact Rakesh Bobba for more information.

**Description of research activity:** This activity aims to develop a methodology that takes cyber-physical dependencies of energy delivery infrastructure into account and assesses the risk of cyber-attack induced cascading failures. This task will be executed in collaboration with other CREDC consortium members and will leverage prior work on cyber-physical models of electrical grid, proposed work on stochastic models for cascading failures, and on analysis of cyber-networks that characterize the difficulty of penetrating them sufficiently to cause an attack. Specifically, in the long-term this task aims to provide real-time situational awareness of threat to the system by characterizing "how far or close" a given grid system is to a cyber-induced cascading failure, and how to mitigate this emergency scenario.

The developed methodology will be validated using realistic cyber-physical models and in available CREDC simulation and emulation test-beds.

**How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?**
The tools and technologies resulting from this work will address the "Assess and Monitor Risk" area of the roadmap by i) providing a framework for assessing vulnerabilities, prioritizing control measures, and means for justifying costs, and ii) providing decision support for security control deployment.

**Summary of EDS gap analysis:** refer to full EDS gap analysis.

**Full EDS gap analysis:** Energy delivery networks such as the electric grid infrastructure critically depend on underlying cyber infrastructure that is vulnerable to cyber attacks. The resilience of the electric grid infrastructure depends on the integrity and availability of the underlying cyber infrastructure. However, current assessment techniques force separate analysis of physical and cyber components. Due to the complexity of protection mechanisms and varying load conditions, it is non-trivial to understand the impact or compute the consequences of cyber-attacks on critical components. We need (i) accurate models/analysis to identify contingency sequences that lead to catastrophic failures such as cascades, (ii) analysis algorithms to identify pathways that trigger such contingencies through cyber-attacks, (iii) metrics to describe the difficulty of penetrating the cyber network, (iv) means of combining cyber and EDS risk into a metric that is meaningful to an operator, and (v) the ability to do this analysis in real-time. The goal is to develop technology such that when the cyber network vulnerability becomes available in real-time (through IDS, observation, or vulnerability report), the system can make a real-time assessment of the impact of that vulnerability, issue an alert, and (ideally) suggest redemptive action. This activity will leverage emerging work on cyber-physical modeling and analysis of grid infrastructure (e.g., [1- 8]) to assess proximity to "cyber-induced cascading failures" much like tools that try to estimate the proximity of the current system operating point to the stability margins in electric grid analysis. For instance, the framework developed in this work can be used for what if analysis including assessing the impact and likelihood of NESCOR failure scenarios (e.g., Generic.2 scenario).

**Bibliography:**

1. K. R. Davis, R. Berthier, S. A. Zonouz, G. Weaver, R. Bobba, E. Rogers, P. W. Sauer, and D. M. Nicol, "***Cyber-Physical Security Assessment (CyPSA) for Electric Power Systems,***" The Bridge, vol. 112, no. 2, May 2016

2. Davis, K.R.; Davis, C.M.; Zonouz, S.; Bobba, R.B.; Berthier, R.; Garcia, L.; Sauer, P.W., "**A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures**," *Smart Grid, IEEE Transactions on ,* vol.6, no.5, pp. 2464 - 2475, Sept. 2015
3. C. W. Ten, A. Ginter and R. Bulbul, "**Cyber-Based Contingency Analysis**," in *IEEE Transactions on Power Systems*, vol. 31, no. 4, pp. 3040-3050, July 2016.
4. C. Vellaithurai, A. Srivastava, S. Zonouz and R. Berthier, "**CPIndex: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructures**," in IEEE Transactions on Smart Grid, vol. 6, no. 2, pp. 566-575, March 2015.
5. Gabriel A. Weaver, Kate Davis, Matt Davis, Edmond J. Rogers, Rakesh B. Bobba, Saman Zonouz, Robin Berthier, Peter W. Sauer, and David M. Nicol, "**Cyber-Physical Models for Power Grid Security Analysis: 8-Substation Case,**" in proceedings of SmartGridComm, 2016., IEEE, November 2016.
6. Y. Zhang, L. Wang, Y. Xiang and C. W. Ten, "**Inclusion of SCADA Cyber Vulnerability in Power System Reliability Assessment Considering Optimal Resources Allocation**," in IEEE Transactions on Power Systems, vol. 31, no. 6, pp. 4379-4394, Nov. 2016.
7. Zonouz, S.; Davis, C.M.; Davis, K.R.; Berthier, R.; Bobba, R.B.; Sanders, W.H., "**SOCCA: A Security-Oriented Cyber-Physical Contingency Analysis in Power Infrastructures**," *Smart Grid, IEEE Transactions on* , vol.5, no.1, pp.3-13, Jan. 2014
8. Zonouz, S.; Rogers, K.M.; Berthier, R.; Bobba, R.B.; Sanders, W.H.; Overbye, T.J., "**SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructures**," *Smart Grid, IEEE Transactions on*, vol.3, no.4, pp.1790-1799, Dec. 2012