Showcase: Industry/Research Partnership: Cyber Resilience Metrics for Bulk Power System

Sachin Shetty, Old Dominion University

Bheshaj Krishnappa, ReliabilityFirst

CREDC Industry Workshop

March 27-29, 2017

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security | cred-c.org

Outline

- Collaborative Research Agreement
- Industry Relevance
- Partnership Establishment
- Research Motivation
- Research Challenges
- Research Approach
- Overcoming Hurdles
- Technology Transition Plan
- Milestones and Deliverables

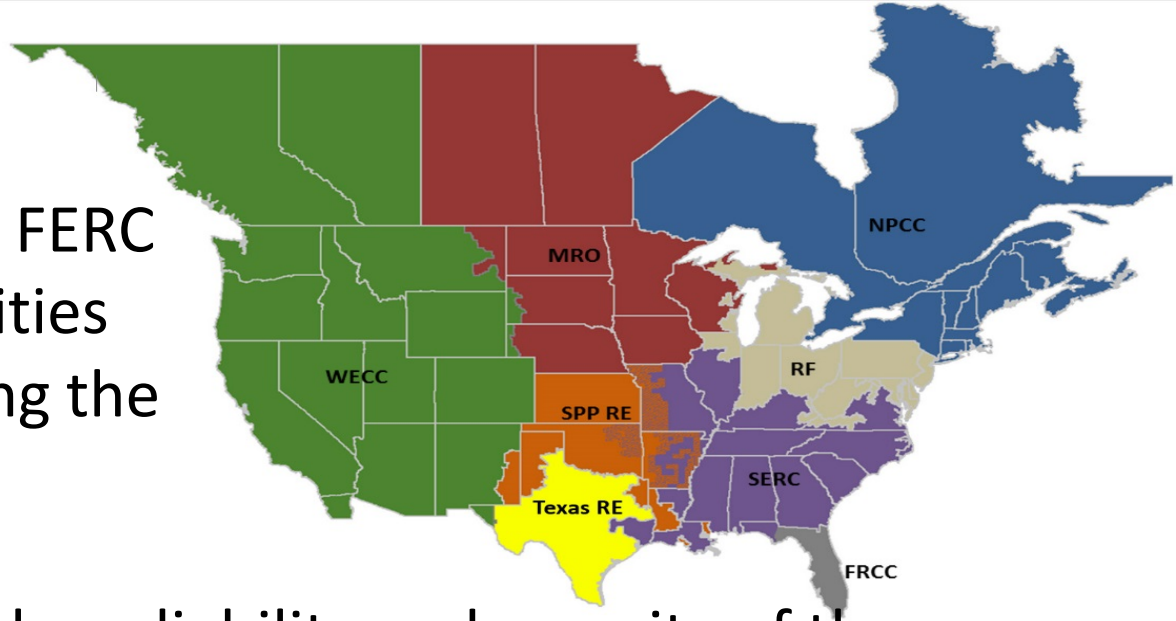
Collaborative Research Agreement

- **Research Agreement Goal**
  - Derive metrics to evaluate cyber resilience
  - ReliabilityFirst (RF) will provide industry knowledge.

- **Research Agreement Purpose**
  - Collaborative project between Old Dominion University and RF to develop cyber resilience metrics for bulk power system
  - Advance RF's mission of promoting grid reliability and resiliency.
  - Provide industry relevance for CREDC research based on data and RF expertise

- **Performance Period** – Q2 2016 – Q2 2017

About RF



- RF is one of the eight FERC approved regional entities responsible for ensuring the reliability of the BPS.

- RF is responsible for the reliability and security of the power system within a footprint which spans 13 states in the Eastern Interconnection.

- Mission involves developing, monitoring, and enforcing compliance with the FERC approved reliability standards for owners, operators and users of the BPS (approximately 230 utilities)
  - Developing and disseminating timely and instructive information to enhance the reliability of the BPS;
  - Provide seasonal and long-term assessments of BPS reliability.

Industry Relevance

- Develop techniques to compute cyber resilience metrics for BPS.

- Opportunity to provide the BPS stakeholders with improved mechanisms or methods to quantify cyber resilience and increase reliability.

- Proposed project will provide methods to quantify and measure cyber resilience.
  - Characterize the ability of the BPS infrastructure to ensure operational resilience in presence of cyber attacks
  - Monitor and simulate scenarios to improve the resilience.

Partnership Establishment

- **Initial Meeting**
  - First CREDC industry workshop, March 2016
- **Follow on Discussions**
  - Several meetings to identify a research project which addresses EDS gaps and relevant to RF and their stakeholders.
- **Research Project Identification**
  - SDN based EDS Risk assessment research activity not a good fit
  - Developed new research activity for BPS cyber resilience metrics
- **Research Collaboration and Work**
  - Established the mechanism between ODU and RF
  - Started working on the project from Q3 2016

Research Motivation

- Availability of BPS cyber resilience metrics will support risk management and mitigation decisions.

- Provide quantitative insights to ensure operational resilience and assist in development of cost-effective mitigation plan.

- Motivate BPS operators to continually assess their resilience capabilities and benchmark their performance

Research Challenges

- Understanding the North American BPS which is a complex technological network comprising of large number of system states, dynamic operating conditions, complex network configurations, wide variety and geographically distributed assets and attack paths

- Existing models for power grid structural resilience focus on graceful degradation in presence of failures, hence the need to quantify graceful degradation

- Quantifying cyber resilience is challenging
  - Resilience of a system depends critically on defining acceptable system performance
  - Cyber resilience metrics for BPS vulnerable to cyber threats needs to be developed
  - Lack of methods to quantify cyber resilience metrics

Research Approach

- Understanding the factors impacting resilience of BPS in terms of availability of essential services
- Utilize and simulate the analytical models to study resilience using the knowledge of BPS Infrastructure, network topologies, firewall configurations, communication technologies, etc.
- Verify and validate the numerical results for BPS cyber resilience metrics
- Measure cyber resilience for power systems as a function of robustness, redundancy, resourcefulness and rapidity.

Research Approach

- *Robustness*—the ability of systems, system elements, and other units of analysis to withstand disaster forces without significant degradation or loss of performance;
- *Redundancy*—the extent to which systems, system elements, or other units are substitutable, that is, capable of satisfying functional requirements, if significant degradation or loss of functionality occurs;
- *Resourcefulness*—the ability to diagnose and prioritize problems and to initiate solutions by identifying and mobilizing material, monetary informational, techno-logical, and human resources; and
- *Rapidity*—the capacity to restore functionality in a timely way, containing losses and avoiding disruptions.

Source: *Bruneau, M., S. E. Chang, R. T. Eguchi, G. C. Lee, T. D. O'Rourke, A. M. Reinhorn, M. Shinozuka, K. Tierney, W. A. Wallace, and D. von Winterfeldt. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. Earthquake Spectra, Vol. 19, No. 4, 2003, pp. 733–752.*

Overcoming Hurdles

- Access to data to validate the proposed theoretical framework

- In our effort, the data requirements were knowledge of BPS Infrastructure, network topologies, firewall configurations, communication technologies, etc.

- We were able to acquire the information that was relevant to validate our technique based on weekly discussions with RF

Technology Transition Plan

- Develop tools to measure robustness, redundancy, rapidity and resourcefulness properties of BPS in the presence of cyber threats.
  - Qualitative - Develop tool which provides BPS operators with a qualitative approach to self-assess the cyber resilience indicators
  - Quantitative – Develop tool which provides cyber resilience metrics for BPS operators based on their operating assets and conditions

Milestones and Deliverables

- **Q4, 2016 –** Completed research paper on graph-theoretic framework to measure cyber resilience of BPS that takes into account the ability to tolerate N-K contingencies.

- **Q2, 2017 –** Preliminary version of qualitative tool to assess security posture of RF stakeholders

- **Q3, 2017 –** Preliminary version of quantitative tool which implements proposed framework to provide cyber resilience metrics for utility companies.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

http://cred-c.org

@credcresearch

facebook.com/credcresearch/

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security