Cyber-Physical Modeling and Visualization for Microgrid Resiliency

Final Project Report

S-82G

Power Systems Engineering Research Center

Empowering Minds to Engineer
the Future Electric Energy System

Cyber-Physical Modeling and Visualization for Microgrid Resiliency

Final Project Report

Project Team

Anurag Srivastava, Project Leader
Adam Hahn
Sajan K. Sadanandan
Washington State University

Graduate Students

Venkatesh Venkataramanan
Partha Sarker
Jonathan Sebastian
Washington State University

PSERC Publication 20-01

March 2020

For information about this project, contact:

Anurag K. Srivastava
The School of Electrical Engineer and Computer Science
Washington State University
Pullman, WA
Phone: 5093352348
Email: anurag.k.srivastava@wsu.edu

Power Systems Engineering Research Center

The Power Systems Engineering Research Center (PSERC) is a multi-university Center conducting research on challenges facing the electric power industry and educating the next generation of power engineers. More information about PSERC can be found at the Center's website: http://www.pserc.org.

For additional information, contact:

Power Systems Engineering Research Center
Arizona State University
527 Engineering Research Center
Tempe, Arizona 85287-5706
Phone: 480-965-1643
Fax: 480-727-2052

Notice Concerning Copyright Material

Acknowledgements

We are thankful to the National Renewable Energy Laboratory (NREL) for funding this important work. We appreciate all the technical support and advice from Brian Miller (NREL). We also acknowledge support from Glen Chason (EPRI), Tony Thomas (NRECA) and Evangelos Farantatos (EPRI) as industry advisors. We are also thankful to PSERC administration and staff for all the necessary logistic support. We would like to acknowledge support from Jayce Gaddis, an undergraduate student at WSU, in developing virtual reality (VR) setup as one of the tasks for this project. Finally, financial support from the US Department of Energy Cyber Resilient Energy Delivery Consortium (CREDC) project is very helpful to augment some of the tool development work discussed in this report.

Executive Summary

The growing prevalence of cyber-attacks on the power system has made it necessary to model the power system as a cyber-physical system. Many of the current systems used to support the electric power grid were designed without the requirement of being resilient to cyber-attacks. A future resilient grid will require that system architectures incorporate attack resilience as a fundamental design requirement. Creating resilient systems designs requires a foundational understanding of attacks and their impacts to the grid. The required understanding is different for transmission power systems, distribution grids and microgrids given their unique features. Microgrids have been getting much traction for its resourceful applicability and scalability. Guaranteeing the energy supply, especially to the critical facilities (e.g. Hospitals and fire department) during extreme outages is essential. With this enhancement, system vulnerabilities and the rising prevalence of cyber-attacks present significant dangers of cyber-physical power grids, especially for a military or critical microgrid. These threats cannot be entirely solved by security mechanisms, the concept of resiliency becomes important for critical infrastructure in cases of extreme contingencies.

The goal of this project is to support a 3D visualization framework for a cyber-physical defense microgrid that will enable the microgrid operator to have enhanced awareness of the operations and command. This research will develop a unique capability to monitor and control cyber and physical microgrid systems to enable increased resiliency for critical loads. This approach will provide a more comprehensive understanding for analyzing the interdependencies between the cyber/control networks and electrical functionality for a variety of microgrid architectures.

The project will leverage the resources and expertise of NREL and WSU with microgrid design and control to integrate the cyber and communication components. Increased consciousness of the microgrid operational status considering all the various layers will enable the operator to take smarter control actions and enable resiliency. In summation, we will propose cyber-physical resiliency metrics that enable the operator to better understand the resiliency of the system. The metrics will consider both cyber and physical system factors and will use an advanced decision-making process to compute metrics that accurately reflect the microgrid resilience in real time.

WSU's microgrid testbed provides a real-time, cyber-physical test environment to model and simulate various cyber-physical attacks and scenarios. WSU's resources include real-time simulation platforms such as RTDS and OPAL-RT, simulation tool such as GridLab-D, openDSS, communication system emulation technologies such as Mininet and various control algorithms that has been developed for microgrid resiliency and control. WSU also has established research focusing on microgrid resiliency metrics, including cyber-physical metrics. This project explored the following specific research goals:

- Cyber-physical microgrid modeling for Miramar Microgrid
- Cyber-physical resiliency analysis and visualization of use cases

This project utilizes system-level simulation studies to explore the impact of failures to specific security mechanisms while also working on to measure and enable resiliency with visualization to identify effective strategies in changing operating scenarios. In this work, cyber-security and cyber resiliency analysis for military microgrid has been presented. Cyber model and interface build on the emerging IEEE 2030.5 protocol for various DERs and microgrids. A framework for interfacing

the protocol with the open source power system analysis software OpenDSS using the REST interface is explained in detail. To examine the potential weaknesses when using the protocol, critical infrastructure such as defense military microgrid are considered. Two military-based microgrid systems - Fort Carson microgrid and Miramar microgrid systems are considered. Simulation results are presented to demonstrate various use cases, including current operational paradigm, and ways of enabling cyber-physical resiliency is explored. A method of measuring resiliency in microgrids is presented and analyzed. By improving situational awareness to take quick and proactive control actions, and by strategically designing the microgrid including various reconfiguration options, the microgrid resiliency can be improved to minimize the impact of cyber-attacks.

Also, use of different visualization tools has enhanced the capability to model micro grid in 3D. Moving forward the biggest challenge with this project will be to tour and model each desired area those represent the microgrid. This will help to build a complete model of microgrid, and operators can have a pseudo real-time experience of operating microgrid while monitoring resiliency of the microgrid for training. We will also use this platform for education and outreach.

The proposed cyber-security and cyber resiliency analysis application is a re-usable models and resources that will effectively bring out the interdependence of the cyber and physical systems of the microgrid. Specifically, microgrid operators will benefit from better understanding of these dependencies and the resulting system resiliency. The proposed microgrid resiliency metrics are also capable of testing and case-study analysis of various microgrid control algorithms and defense techniques. Publications resulted from this work is under review and one accepted.

Technical Publication:

[1] P. Sarker, V. Venkataramanan, D. Sebastian Cardenas, A. Srivastava, A. Hahn, and B. Miller, “Cyber-Physical Security and Resiliency Analysis Testbed for Critical Microgrids with IEEE 2030.5”, IEEE/ ACM CPSWeek, MSCPES workshop, Sydney, Australia, April, 2020

Student Thesis:

[2] Venkatesh Venkataramanan. “Cyber-Physical Resilience Assessment for Active Power Distribution Systems”, Ph.D. Thesis, Washington State University, July 2019.