Reliability Assessment and Modeling of Cyber Enabled Power Systems with Renewable Sources and Energy Storage

Final Project Report

T-53

Power Systems Engineering Research Center
Empowering Minds to Engineer the Future Electric Energy System
Reliability Assessment and Modeling of Cyber Enabled Power Systems with Renewable Sources and Energy Storage (T-53)

Final Project Report

Project Team

Chanan Singh, Project Leader
Alex Sprintson
Texas A&M University

Visvakumar Aravinthan
Wichita State University

PSERC Publication #16-07

November 2016
For information about this project, contact

Chanan Singh
Regents Professor and Irma Runyon Chair Professor
Department of Electrical and Computer Engineering
Texas A&M University
3128 TAMU
College Station, Texas 77843-3128
Email: singh@ece.tamu.edu
Phone: 979-845-7589

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: 480-965-0745

Notice Concerning Copyright Material

PSERC members are given permission to copy without fee all or part of this publication for internal use if appropriate attribution is given to this document as the source material. This report is available for downloading from the PSERC website.

© 2016 Texas A&M University. All rights reserved.
Acknowledgements

This is the final report for the Power Systems Engineering Research Center (PSERC) research project titled “Reliability Assessment and Modeling of Cyber Enabled Power Systems with Renewable Sources and Energy Storage” (project T-53). We express our appreciation for the support provided by PSERC’s industry members and by the National Science Foundation under the Industry / University Cooperative Research Center program.

We wish to thank the following Industry Team Members whose advice we acknowledge: M. J. Mousavi, ABB Inc.; J. Fleeman, AEP; K. D. Phillips, AEP; M. Shao, GE Energy Management; W. Li, BC Hydro; X. Luo, ISO New England; L. Min, Lawrence Livermore National Lab; D. Arjona, Idaho Power; and M. Papic, Idaho Power; Adam Wigington, EPRI.
Executive Summary
Quantitative reliability indices are important to utility companies, vendors, and regulators for planning, operation, maintenance, and regulatory purposes. System reliability evaluation methodologies have been mostly focusing on the current-carrying part which is called physical part in this report and the cyber part is assumed to be perfectly reliable in these evaluations. As a part of the efforts to make the grid smarter, the cyber part has been rapidly expanding. The term “cyber” refers to the devices and activities residing in the secondary side of the power system, associated with the functionalities of measurement, control, monitoring, and protection. The overall power system is also referred to as a “cyber-physical power system”, in which the communication networks and power components are interdependent. The cyber-physical interdependencies exist extensively in power systems at all levels and associate with various aspects. The main focus of this work is to investigate this cyber-physical interdependence and develop methods for evaluation of reliability considering this mutual relationship. There are three sections in this report. Part I is concerned with modeling of interdependence between cyber and physical at the composite system level and Part II is focused at the distribution level. During the course of these investigations we also developed a new efficient algorithm for approximating failure frequency with provable guarantees that can be used both for the physical and cyber parts and this is described in Part III.

Part I. Reliability Modeling and Analysis of Cyber Enabled Power Transmission Systems
Information and Communication Technologies (ICTs) are becoming more pervasive in electric power systems to improve system control, protection, monitoring, and data processing capabilities. Generally the ICT technologies are assumed to be perfectly reliable in the process of composite power system reliability evaluation. The failure of these technologies, however, can widen the scope and impact of the failures in the current carrying part. This assumption may thus have significant effect on the reliability indices calculated and result in too optimistic reliability evaluation. For realistic reliability evaluation, it is necessary to consider ICT failures and their impact on composite power systems.

We have extended the scope of bulk power system reliability modeling and analysis with the consideration of cyber elements. Analysis of composite power system together with the cyber part can become computationally challenging. A novel computationally tractable methodology with the use of Cyber-Physical Interface Matrix (CPIM) is proposed and demonstrated. The CPIM decouples the analysis of cyber system from the evaluation of the physical system and provides the means of performing the overall analysis in a manageable fashion.

Using the concept of Cyber-Physical Interface Matrix (CPIM), we perform reliability modeling and analysis at the substation level. We have enhanced the substation model with consideration of cyber-link failures. In an attempt to use a non-sequential MCS for dependent failures induced by the cyber failures, we investigate the major difficulties of applying conventional non-sequential sampling methods to generating appropriate state space in the presence of dependent failures and propose a method to overcome these difficulties.

Part II. Reliability Assessment and Modeling of Cyber Enabled Power Distribution Systems
The distribution system reliability evaluation in presence of cyber system is modeled and analyzed in this work. The primary focus of this work has two directions:
a) Distribution System Reliability Evaluation
This part focuses on developing a reliability evaluation technique that is scalable and could be utilized in multi system framework. The proposed model utilizes failure modes and effects analysis and reduces computational complexity using branch and node information of the network. Load point based model is used to preserve topology information and include cyber network in the next part.

b) Cyber-Power System based Reliability Modeling and Analysis
This part focuses on incorporating the properties of cyber – physical systems to develop a reliability evaluation model. Two types of cyber failures (i) cyber unavailability and (ii) cyber-attacks are considered in this work to determine system reliability. Fault detector and automated switch placement as considered as example applications in this work.

Part III. An Efficient Algorithm for Approximating Failure Frequency with Provable Guarantees
In this work, we consider the problem of approximating the failure frequency of large-scale composite systems whose terminals are connected through components that experience random failure and repair processes over time. At any given time, a system failure occurs if the surviving system fails to have all-terminal connectivity. We assume that each component’s up-times and down-times are modeled by statistically independent stationary random processes, and these processes are statistically independent across the components. In this setting, the exact computation of failure frequency is known to be computationally intractable (NP-hard). This work, for the first time, provides a polynomial-time algorithm to approximate the failure frequency with high probability within an arbitrary multiplicative error factor using near-minimum cut sets. Moreover, our numerical results show that not only is the proposed method computationally more efficient than the commonly-used bounding technique, but it also has a superior performance in terms of the accuracy of the approximation.

Principal Outcomes
1. Developed a reliability evaluation methodology for composite power systems using Cyber-Physical Interface Matrix (CPIM) and Consequent Events Matrix (CEM) that decouple the analysis of cyber from the physical part.
2. Illustration of the methodology on an extended standard reliability test system for system-wide reliability analysis.
3. A non-sequential Monte Carlo approach for systems having dependent failures induced by cyber failures.
4. A new approach to calculation of frequency of failure using cut sets.
6. Identification of ways emerging cyber enabled devices and logics put power system at risk. These vulnerabilities are categorized into unavailability of data and cyber security threats.

7. Investigation of the necessity of updating the traditional reliability models to incorporate cyber enabled logic. The developed model leads to more accurate and realistic reliability indices at distribution feeder level.

8. Common mode failures are introduced as a potential vulnerability in cyber enabled power distribution network as multiple devices can fail due to a common cause.

9. The proposed probabilistic model is incorporated into a traditional power distribution network planning problem to illustrate the effectiveness of the developed model.

Project Publications


