2014 IEEE 38th Annual International Computers, Software and Applications Conference

Analysis of Reliability and Resilience for Smart Grids

Murtadha N. Albasrawi, Nathan Jarus, Kamlesh A. Joshi, and Sahra Sedigh Sarvestani
Department of Electrical and Computer Engineering
Missouri University of Science and Technology, Rolla, MO 65409, USA
Email: {mnaky2,kaj998,nmjxv3,sedighs}@mst.edu

***Abstract*—Smart grids, where cyber infrastructure is used to make power distribution more dependable and efficient, are prime examples of modern infrastructure systems. The cyber infrastructure provides monitoring and decision support intended to increase the dependability and efficiency of the system. This comes at the cost of vulnerability to accidental failures and malicious attacks, due to the greater extent of virtual and physical interconnection. Any failure can propagate more quickly and extensively, and as such, the net result could be lowered reliability. In this paper, we describe metrics for assessment of two phases of smart grid operation: the duration before a failure occurs, and the recovery phase after an inevitable failure. The former is characterized by reliability, which we determine based on information about cascading failures. The latter is quantified using resilience, which can in turn facilitate comparison of recovery strategies. We illustrate the application of these metrics to a smart grid based on the IEEE 9-bus test system.**

Keywords*—reliability; resilience; analytical model; smart grid; cyber-physical;

I. Introduction

Recent blackouts attest to the need for measures to predict and assess the reliability of power grids. The August 2003 Northeast blackout affected nearly 50 million customers in seven US states and Ontario. Rigorous investigation of the cause determined that aging infrastructure, lack of real-time information and diagnostic support, local decision-making without regard to interconnectivity, and human error allowed localized failure of a generating plant to force the shutdown of over 100 power plants [1]. The source of the cascade was contact of stressed power lines with overgrown trees - a failure whose effects could have been mitigated given intelligent and real-time diagnostic support that would reconfigure adjacent power grids to prevent propagation of the failure.

Eight years later, in August 2011, a blackout affected nearly three million customers near San Diego. The causes were judged to be strikingly similar to those of the 2003 blackout, despite significant activity by regulatory bodies in an attempt to prevent outages similar to what occurred in 2003 [2]. Recent large-scale and high-consequence outages in several other countries, including India and Brazil, attest to the importance of predicting, preventing, and mitigating the effects of cascading failures. Complete replacement of aging infrastructure is infeasible; however, use of cyber infrastructure can equip power grids with the information required for prompt detection and diagnosis, and the ability to limit failure propagation. Monitoring capabilities and intelligent control are among the essential attributes of smart grids, which are intended to increase the dependability and sustainability of power distribution. The communication, computing, and control elements required to embed the power grid with the required intelligence make smart grids more complex than their purely physical counterparts. Each added component is a potential source of failure, and the increased connectivity of the grid makes failure propagation more likely. Assessment, modeling, and prediction of the reliability of smart grids is critical to justifiable reliance on these systems. As failures are inevitable, techniques are required to guide recovery.

In this paper, we propose solutions to both challenges and illustrate the application of our techniques on a small smart grid based on the IEEE 9-bus test system. Utilizing simulation, we derive information about potential cascading failures and use this information to populate the stochastic reliability model proposed in our earlier work [3]. Our prior work considered a larger grid, but was constrained in application. The first contribution of this paper is extension of the previous model to allow for consideration of a richer set of intelligent devices in determining reliability of the smart grid. The simulation framework through which our case study was conducted facilitates future analysis of survivability by allowing for degraded levels of functionality. Instead of the hardware-in-the-loop simulator that bound us to a specific topology and specific cyber infrastructure, the current simulation framework allows for analysis of arbitrary physical and cyber-physical topologies, and facilitates fine-grained fault injection. In determining reliability, our focus is on the consequences of a specific failure, not its cause. As such, the technique can be utilized in security analysis.

Reliability quantifies the likelihood of a system to function as specified, under given conditions, over a given duration [4]. It takes a binary view of a system, where the only states possible are "functional" and "failed." As such, this metric is of limited use in evaluating the system after a failure occurs. A quantitative metric useful to this end is "resilience," defined as the ability of a system to bounce back from a failure [5]. The second contribution of this paper is identification of performance indices appropriate for analysis of resilience, and using the resulting resilience metric to compare strategies for recovery from line failures in the IEEE 9-bus system.

The metrics we with which we capture reliability and resilience, respectively, are presented in Section II. As a case study, application of these metrics to the IEEE 9-bus is illustrated in Section III. Section IV positions our work in the context of related literature. Section V concludes the paper and describes future extensions planned for this research.

0730-3157/14 $31.00 © 2014 IEEE
DOI 10.1109/COMPSAC.2014.75

II. METRICS

In this section, we describe metrics and techniques for modeling of reliability and resilience, respectively. Our view of the system's operation is based on [5] and [6] and illustrated in Figure 1. The system is initially "functional," at time t_0. This perspective is consistent with the view taken in evaluating system reliability - the system is considered to be binary in operation; it either works or has failed. The extent of functionality is not of interest in determining reliability. Some quantifiable indicator of the performance of the system is selected as the *figure of merit*, $F(t)$, and monitored over time. If $F(t)$ exceeds a minimum threshold, the system is considered functional. A failure (denoted as a "disruptive event" in [6]) occurs at time t_e. For simplicity, we assume that the failure is detected instantaneously and the system is immediately considered to have failed. Analysis of reliability can capture the duration between t_0 and t_e - once the system has failed, it leaves the purview of reliability analysis, which is incapable of capturing degraded operation or recovery. Availability, resilience, and survivability can capture the state of the system after a failure.

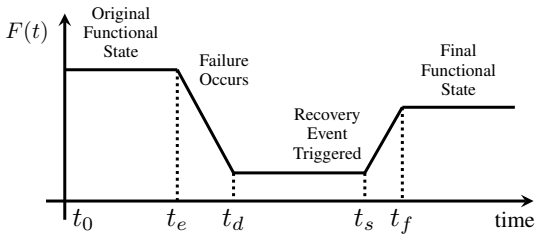

Fig. 1. System operation over time.

In Figure 1, the system is assumed to function in a degraded mode from t_e to t_d, when it reaches the point where the functionality is considered to be entirely lost, rather than degraded. Recovery/repair is initiated at time t_s, when the system regains functionality, albeit in a degraded state. At t_f, the system is assumed to be back in the fully-functional state that is the subject of reliability analysis. Availability captures the ratio of "up time" to "down time." Survivability quantifies degraded performance. Resilience, the second metric discussed in this paper, captures the ability of the system to recover from a failure; i.e., the success of recovery efforts [4]. The remainder of this section describes our approach to quantifying the reliability and resilience of a system.

A. Reliability

The overall reliability of a cyber-physical power grid is a function of the respective reliabilities of its elements, including both physical components, e.g., generators and transmission lines, and cyber components, e.g., control software, communication links, FACTS devices, and sensors. As such, we chose the Markov Imbeddable Structure (MIS) technique [7] - an analytical method for reliability evaluation of systems with interdependent components - as the mathematical foundation for our proposed reliability model. Our past and current work have this foundation in common; they differ considerably in the scope of components (and hence failures) considered.

The MIS model requires identification of "Functional" and "Failed" states of the system, and computes the system reliability as the probability of being in one of the "Functional" states. We explain the MIS technique using an example. Assume that we have a system that has $n = 2$ transmission lines. The state of each transmission line is represented by a '1' when it is functional and a '0' otherwise. Enumerating all states of the system results in the matrix of Table I.

TABLE I. ENUMERATION OF SYSTEM STATES

	Components	
States	l_1	l_2
S_0	1	1
S_1	1	0
S_2	0	1
S_3	0	0

Next, we create a vector of probabilities, $\mathbf{\Pi_0}$, where element i represents the probability of state S_i being the initial state of the system. With n components, $N = 2^n$ states are possible.

$$\mathbf{\Pi_0} = [Pr(Y_0 = S_0), Pr(Y_0 = S_1), \cdots, Pr(Y_0 = S_N)]^T \tag{1}$$

We also create a transition probability matrix, P_l. Each element in the matrix, $p_{ij}(l)$, is the probability of the system changing its state from state S_i to state S_j due to the failure of transmission line l. For example, in Table I, when transmission line l_1 fails, the state of the system will change from S_0 to S_2. The probability will be of this transition is 1, because the failure of l_1 is certain to cause an initially functional system (in state S_0) to transition to S_2.

Finally, we create a vector, **u**, of length 2^n. Element **u[i]** in the vector depends on state S_i in the binary matrix. If state S_i is considered a functional state, then **u[i]** will be '1', otherwise, it will be '0'. Collectively, the matrices and vectors defined enable determination of system-level reliability as a function of the respective reliabilities of components of the system, as in Equation 2.

$$R = (\mathbf{\Pi_0})^T \left(\prod_{l=\mathbf{1}}^{n} \mathbf{P}_l \right) \mathbf{u} \tag{2}$$

B. Resilience

Resilience quantifies the ability of a system to recover from a failure. Recovery does not imply perfect restoration of the system's functionality - it implies that the system has returned to a state where it is considered functional. As described earlier in this paper, a quantifiable aspect of the performance of the system is evaluated at the significant time points illustrated in Figure 1. Examples include the total number of voltage or current violations in a power grid, or the percentage of the overall power demand that can be met. We assume that the system begins with full functionality, denoted as $F(t_0)$. The failure event causes the performance to degrade. $F(t_d)$ is the value at which catastrophic failure is considered to have occurred. The system performance remains in this catastrophic state until recovery action is initiated at time t_s, when partial functionality begins to be restored. $F(t_f)$ is considered to be acceptable functionality - the system may not return to the

perfectly functional state, but it delivers performance that is deemed acceptable. Resilience captures this recovery process as a ratio of recovered functionality to lost functionality. Mathematically, for a given instant t during the recovery process (t_s, t_f) from a specific failure:

$$\Lambda(t) = \frac{F(t) - F(t_d)}{F(t_0) - F(t_d)} \tag{3}$$

It follows that $0 \leq \Lambda(t) \leq 1$ for all $t \in (t_s, t_f)$, assuming that the recovery action succeeds in restoring functionality.

III. Case Study

As a case study, we illustrate modeling and evaluation of reliability and resilience, respectively, for the IEEE 9-bus system. This test system represents a portion of the Western System Coordinating Council (WSCC) 3-Machines 9-Bus system and includes nine buses, nine transmission systems, three generators, and three loads. Figure 2 depicts the grid in its purely physical form. Bus 1 is assumed to be the reference/slack bus.

Our motivation for selection of this test system is twofold. The first benefit is the simplicity of the grid, which facilitates illustration of concepts. The second benefit is that this system has been the topic of several other studies, e.g., [9], [10]. The results can serve as benchmarks for parts of our analysis.

For our case study, we used the Power System Analysis Toolbox (PSAT) and PowerWorld, respectively, to simulate the IEEE 9-bus system. PSAT is an open-source MATLAB-based software package for analysis and design of electric power systems [11]. PSAT supports a number of electronic control devices and allows fault injection and manipulation of information exchange between components. PowerWorld is a proprietary simulation environment for high-voltage power systems.

A. Reliability Analysis

In deriving a system-level reliability model for the IEEE 9-bus system, we began with the purely physical infrastructure of Figure 2. Using PSAT, we simulated single-line contingencies; i.e., outage of each of the nine transmission lines. The outage of lines (2-7), (3-9), and (1-4), respectively, triggered cascading failures. In this notation, the two numbers in the parentheses are the buses connected by the line in question. Outage of any one of the six remaining transmission lines was not found to trigger a cascade. In applying the MIS model of Equation 2, we consider the system to be functional despite the outage of a single line if a cascade is not triggered. Hence:

$$R_{sys} = p_L^9 + 6p_L^8 q_L \tag{4}$$

In Equation 4, the reliability of a transmission line is represented by $p_L = 1 - q_L$. For tractability, all lines have been considered equally reliable.

To determine the effect of intelligent control on reliability of the system, we added one Static Synchronous Series Compensator (SSSC) device to the system. An SSSC is a computer-controlled power electronics (FACTS) device that is connected in series with the AC system. The output current of the SSSC is adjusted to control the nodal voltage magnitude. The failure of an SSSC device could initiate cascading failures. The configuration parameter that controls the power flow in the system is *Percentage amount of series compensation* (PASC), which ranges from 0 to 99. An SSSC will function as a breaker if this parameter is set to 0.

Due to the small size of the system, we opted to use a single SSSC for intelligent control of the resulting smart grid. Optimal placement of the SSSC can be determined by exhaustive search for a system of this size. The results of this simulation fell into three groups. In the first group, using the SSSC decreased the reliability of the system, even if the PASC value was optimal. Addition of the SSSC did not change the

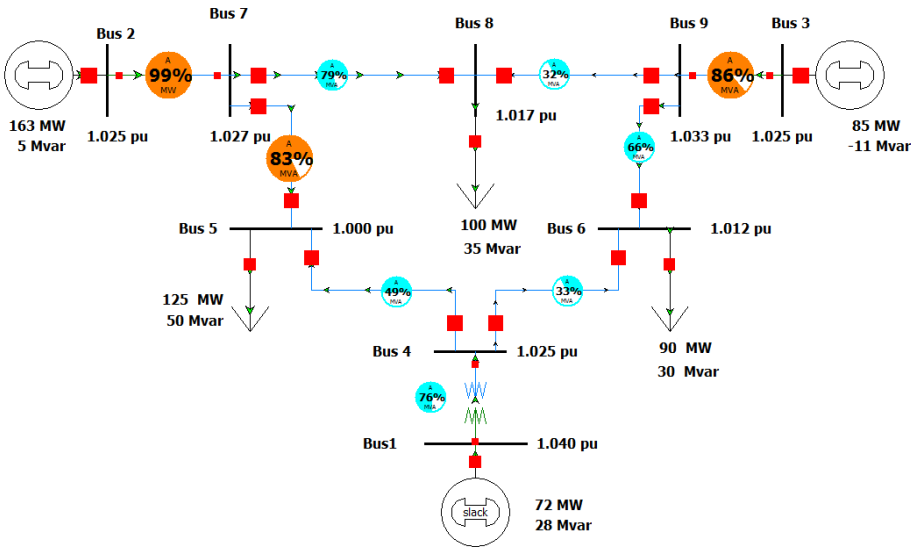

Fig. 2. IEEE 9-Bus System (figure adapted from [8])

reliability of the system in the second group, regardless of the PASC. The third group is where the goal of increasing reliability is actually achieved. Placing an SSSC with a PASC value ranging between 49 to 61 on line (8-9) was found to decrease the number of potential cascading failures from three to two. Placing an SSSC with a PASC value between 15 and 34 on line (5-7) had an identical effect.

Assuming that the SSSC is perfect, the reliability of the smart grid can be determined using Equation 2:

$$R_{sys} = p_L^9 + 7p_L^8 q_L \tag{5}$$

A more realistic assumption is that the SSSC itself is prone to failure. Denoting its reliability as p_{SSSC}, the overall reliability of the smart grid can be modeled as:

$$R_{sys} = (p_L^9 + 6 * p_L^8 q_L) * p_{SSSC} + \sum_{\forall states \in S} p_L^8 q_L * p_{SSSC} \tag{6}$$

where S is the set of states where a cascading failure would have occurred without an SSSC, but is prevented by its addition (and correct configuration), and p_{SSSC} is the reliability of the SSSC device.

Figure 3 illustrates the results of our simulation. It is evident that only a very reliable SSSC improves the system reliability beyond that of the purely physical grid.

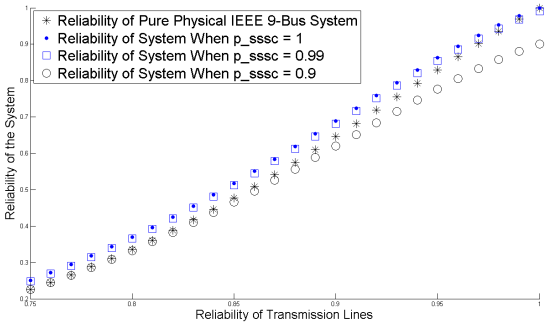

Fig. 3. Effect of SSSC on overall smart grid reliability

B. Resilience Analysis

In analyzing resilience, one of our objectives was to determine the best strategy to recover from multiple failures. Contrary to the reliability example, the line outages considered are not necessarily the result of a cascade - they could occur independently.

The first step in evaluating the resilience of the system is selecting an appropriate quantifiable measure of functionality. Violations of power flow and voltage constraints are typical measures of the extent of disruption to a power grid. We carried out contingency analysis by causing the outage of three transmission lines on a common bus and observing the resulting number of power flow and voltage violations. For brevity, we discuss only the most severe failure: an outage of lines (2-7), (5-7), and (7-8), which results in 11 violations (7 voltage and 4 power flow).

Contingency analysis demonstrated that for three-line disruptions, the maximum flow violation occurs on line (1-4), where the rated apparent power limit is exceeded by 239%. Thus, we selected the power flow on line (1-4) as our first measure of functionality, F_1. Further, in examining bus voltage violations, we found that bus 8 experiences the lowest voltage (0.968 power units (pu)) in response to the outage. The voltage of bus 8 was selected as the second measure of functionality, F_2.

We compare the following two strategies for recovery from the outage:

- Strategy 1: Recover lines 7-8, 5-7, and 2-7, in order
- Strategy 2: Recover lines 5-7, 7-8, and 2-7, in order

Equation 3 is used to calculate the resilience, based on F_1 and F_2, respectively. When the grid is functional, F_1 = 76% and F_2 = 1.017 pu.

In comparing the two recovery strategies, we assume that lines can be repaired one-at-a-time. Referring to Figure 1, the first repair is initiated at time t_s. t_1 and t_2 indicate the beginning of the intermediate repair steps. The final (in this case, third) repair is completed at time t_f, when the system is assumed to have returned to a functional state. We assume that the repair of each of the three lines takes equally long, and that this repair time is a known (deterministic) value. This assumption will be relaxed in future work.

Tables II and III, respectively, show the values of the two functional metrics, F_1 and F_2, and the respective resilience values, Λ_1 and Λ_2, achieved by the two strategies examined.

TABLE II. RESILIENCE IN RECOVERY, USING STRATEGY 1

Metric	Time					
	t_0	t_d	t_s	t_1	t_2	t_f
F_1	76	239	239	238	235	76
Λ_1	1	0	0	0.006	0.024	1
F_2	1.017	0.968	0.968	0.992	1.007	1.017
Λ_2	1	0	0	0.490	0.796	1

TABLE III. RESILIENCE IN RECOVERY, USING STRATEGY 2

Metric	Time					
	t_0	t_d	t_s	t_1	t_2	t_f
F_1	76	239	239	235	235	76
Λ_1	1	0	0	0.02454	0.02454	1
F_2	1.017	0.968	0.968	0.972	1.007	1.017
Λ_2	1	0	0	0.0817	0.796	1

The resilience values can be used to select a restoration strategy. Figure 4 compares the resilience, as calculated based on F_2, for recovery using each of the two strategies. Strategy 1 proves to be a better option, as it builds resilience faster; after line (7-8) is recovered, the voltage on bus 8 increases from 0.968 pu to 0.992 pu, yielding a resilience value of $\sim$0.490.

Both strategies yield almost identical results when resilience is calculated based on flow violations (F_1), and as such, this functional metric cannot be used to compare strategies. Since the second strategy yields better results for Λ_1, it is recommended for recovery.

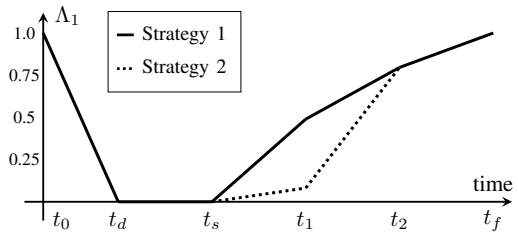

Fig. 4. Line Flow Resilience (Λ_1) in Recovery

IV. Related Work

Cascading failures, defined as "the usual mechanism by which failures propagate to cause large blackouts of electric power transmission systems," are a major cause of widespread outages in the power grid [12]. Relevant studies propose models for the propagation of hidden failures, and suggest mitigation techniques based on configuration of control devices [13], [14]. In [15], the authors developed a DC power flow model to study the effect of the topology of the power grid on failure propagation. The intuitive conclusion reached was that increased connectivity can delay cascading, but reduced connectivity can lead to improved performance during contingencies. The effect of using local power sources was investigated in [16], where simulation was used to demonstrate that local power sources can reduce the probability of cascading failure. The role of the depth of cascading failures on robustness of the network was investigated in [17]. They showed that system robustness increases when the grid can tolerate deeper cascading failures and decreases when the system fails quickly.

Contingency, defined as the failure of a device, e.g., a line or transformer, is one cause of failures in power grids. Studies such as [18] investigate the effect of line contingencies on cascading failure and determine "importance" values for each line. This study, as the vast majority of related studies, considers a purely physical infrastructure. The addition of power electronics devices that can control the flow of power on a given line and prevent or mitigate the effect of contingencies creates a cyber-physical power infrastructure. One type of intelligent device used to this end is a Thyristor-Controlled Series Capacitor (TCSC). The success of such devices in preventing and mitigating cascading failures has been demonstrated in several studies, including [19], [20], [21]. These studies illustrated the impact of prudent location of the TCSC on load management and distribution during a contingency. The broader category of Flexible AC Transmission Systems (FACTS), which can be considered to comprise TCSCs, has been investigated in studies such as [22], [23]. Both studies proposed techniques for optimal placement of FACTS and algorithms for determination of the best settings for the devices.

The work most closely related to the research presented in this paper considers quantitative modeling of the reliability of physical (vs. cyber-physical) power systems. Examples include [24], which mainly focuses on reliability of power transmission systems, and [25] which describes an analytical approach and a Monte Carlo simulation technique for evaluating the reliability indices of distribution systems. A graph-theoretical model for reliability, and subsequent importance analysis of a power grid is presented in [26]. Our model for reliability considers the effect of failures in the cyber infrastructure in the overall likelihood of a cascading failure.

A second category of related work investigates techniques for evaluating and increasing the resilience of networked systems. Related studies often include importance analysis, as one objective is to determine recovery strategies. A Markov reward model is used for importance analysis in [27]. A more detailed analysis is carried out in [28], where three importance indices are defined. The first metric is the Failure Criticality Index, which ranks the importance of components based on a parameter of interest. The Restore Criticality Index is the second metric, which assesses the impact of restoration of a specific component. The third and final metric is the Operation Criticality Index, defined as the ratio of component downtime to system downtime.

Our work on resilience is based on the metrics and analysis proposed in [5] and [6]. Their analysis of component vulnerability is similar to that of [29], which investigated the importance of a component in a network by determining the efficiency of the network during the failure of a single component. The goal of [29] was to determine improvements to the system that will considerably increase this efficiency. Our work applies the approach of [5] and [6] in comparing recovery strategies for a power grid, where the goal is to achieve the highest resilience possible; i.e., regain acceptable functionality as rapidly as possible. From the recovery point of view, related work includes [30], where a congestion management technique was introduced in order to decrease the financial losses incurred during contingency; and [31], where concurrent monitoring of providers and customers was carried out manage and predict contingencies caused by sudden load increases.

V. Conclusion

The overarching objective of the work presented in this paper is to enable assessment of the capability of a power grid to deliver the functionality expected. We sought to select measures that collectively assess this capability during both normal and degraded system operation - before, after, and during recovery from a failure event. Reliability quantifies the probability that a system will deliver acceptable functionality under given conditions, over a given duration. We presented a Markovian reliability model that calculates this probability based on the reliability of constituent components of the system and enumeration of "functional" and "failed" system states. We demonstrated application of this reliability model to the IEEE 9-bus test system, both with and without an intelligent control device. We carried out single-line contingency analysis, and considered the system functional whenever the line outage did not result in cascading failure. The results reinforced an intuitive conclusion - that only very reliable intelligent control can improve an already reliable physical infrastructure.

Reliability is incapable of assessing degraded functionality. As such, we selected resilience as the metric to be used in evaluating the system after a failure has occurred. Resilience captures the ability of the system to recover from catastrophic failure and return to a state where it is considered functional. More specifically, it is the ratio of recovered functionality to

lost functionality. Evaluation of resilience requires selection of a quantitative functional metric. In our analysis of the IEEE 9-bus system, we selected line flow violations and voltage violations, respectively, as two functional metrics used in calculation of resilience. We compared the resilience achieved using different recovery strategies for restoration of transmission lines whose outage had led to catastrophic failure of the grid. This type of analysis can be invaluable in decision support for real-time failure mitigation.

Our techniques for analyzing reliability and resiliency are not specific to power grid systems. They can be applied to many fields, including other critical infrastructures, and even software engineering. Both techniques can scale to systems much more complex than the examples in this paper.

Future extensions to the work presented include investigation of the effect of intelligent control on resilience of a power grid, importance analysis of various components of a smart grid, consideration of non-determinism in restorative actions, and bounding the time before recovery actions are attempted. Modeling of system survivability, availability, and recovery are also planned. Finally, the proposed techniques will be applied to significantly larger and more complex smart grids, possibly in an iterative fashion.

REFERENCES

[1] U.S.-Canada Power System Outage Task Force, "Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations," tech. rep., Apr. 2012.

[2] Federal Energy Regulatory Commission and North American Electric Reliability Corporation, "Final report on the Arizona-Southern California outages on September 8, 2011," tech. rep., Apr. 2004.

[3] A. Faza, S. Sedigh, and B. McMillin, "Integrated cyber-physical fault injection for reliability analysis of the smart grid," in *Proc. of the 29th International Conference on Computer Safety, Reliability and Security (SAFECOMP '10)*, (Vienna, Austria), pp. 277–290, Sept. 2010.

[4] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, pp. 11–33, Jan.-Mar. 2004.

[5] D. Henry and J. E. Ramirez-Marquez, "Generic metrics and quantitative approaches for system resilience as a function of time," *Reliability Engineering & System Safety*, vol. 99, pp. 114 – 122, 2012.

[6] K. Barker, J. E. Ramirez-Marquez, and C. M. Rocco, "Resilience-based network component importance measures," *Reliability Engineering & System Safety*, vol. 117, no. 0, pp. 89 – 97, 2013.

[7] W. Kuo and M. J. Zuo, *Optimal Reliability Modeling, Principles and Applications*, pp. 164–171. John Wiley and Sons, Inc., Hoboken, New Jersey, 2003.

[8] Illinois Center for a Smarter Electric Grid (ICSEG), "Case 1 - IEEE 9 Bus Systems." http://publish.illinois.edu/smartergrid/case-1-ieee-9-bus-systems/, Apr 23, 2014.

[9] Z.-G. Wu, Q. Zhong, and Y. Zhang, "State transition graph of cascading electrical power grids," in *Proc. of the IEEE Power Engineering Society General Meeting*, pp. 1–7, June 2007.

[10] J.-H. Heo, M.-K. Kim, G.-P. Park, Y.-T. Yoon, J.-K. Park, S.-S. Lee, and D.-H. Kim, "A reliability-centered approach to an optimal maintenance strategy in transmission systems using a genetic algorithm," *IEEE Transactions on Power Delivery*, vol. 26, pp. 2171–2179, Oct 2011.

[11] F. Milano, "An open source Power System Analysis Toolbox," *IEEE Transactions on Power Systems*, vol. 20, pp. 1199–1206, Aug. 2005.

[12] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman, "Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 17, no. 2, p. 026103, 2007.

[13] D. Pepyne, C. Panayiotou, C. Cassandras, and Y.-C. Ho, "Vulnerability assessment and allocation of protection resources in power systems," in *Proc. of the American Control Conference*, vol. 6, pp. 4705–4710 vol.6, 2001.

[14] J. Chen, J. Thorp, and I. Dobson, "Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model," *International Journal of Electrical Power and Energy Systems*, vol. 27, no. 4, pp. 318–326, 2005.

[15] D. L. Pepyne, "Topology and cascading line outages in power grids," *Journal of Systems Science and Systems Engineering*, vol. 16, no. 2, pp. 202–221, 2007.

[16] X. Chen, H. Dinh, and B. Wang, "Cascading failures in smart grid - benefits of distributed generation," in *Proc. of the IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 73–78, 2010.

[17] M. Youssef, C. Scoglio, and S. Pahwa, "Robustness measure for power grids with respect to cascading failures," in *Proc. of the International Workshop on Modeling, Analysis, and Control of Complex Networks (CNET)*, pp. 45–49, ITCP, 2011.

[18] M. Moghavvemi and O. Faruque, "Real-time contingency evaluation and ranking technique," *IEE Proceedings on Generation, Transmission and Distribution*, vol. 145, no. 5, pp. 517–524, 1998.

[19] S. Slochanal, M. Saravanan, and A. Devi, "Application of PSO technique to find optimal settings of TCSC for static security enhancement considering installation cost," in *Proc. of the 7th International Power Engineering Conference (IPEC)*, pp. 1–394, 2005.

[20] G. Rashed, H. I. Shaheen, and S. Cheng, "Evolutionary optimization techniques for optimal location and parameter settings of TCSC under single-line contingency," in *Proc. of the IEEE Power and Energy Society General Meeting*, pp. 1–9, 2008.

[21] A. Othman, M. Lehtonen, and M. El-Arini, "Enhancing the contingency performance of HELENSÄHKÖVERKKO OY 110 KV network by optimal installation of UPFC based on genetics algorithm," in *Proc. of the IEEE Power and Energy Society General Meeting*, pp. 1–8, 2010.

[22] A. Lininger, B. McMillin, M. Crow, and B. Chowdhury, "Use of Max-Flow on FACTS devices," in *Proc. of the 39th North American Power Symposium (NAPS)*, pp. 288–294, Sept 2007.

[23] J. Chaloupek, D. Tauritz, B. McMillin, and M. Crow, "Evolutionary optimization of flexible A/C transmission system device placement for increasing power grid reliability," in *Proc. of the 6th International Workshop on Frontiers in Evolutionary Algorithms (FEA)*, (Salt Lake City, Utah), pp. 516–519, Nov. 2005.

[24] C. Dichirico and C. Singh, "Reliability analysis of transmission lines with common mode failures when repair times are arbitrarily distributed," *IEEE Transactions on Power Systems*, vol. 3, pp. 1012–1019, Aug. 1988.

[25] S. Asgarpoor and M. Mathine, "Reliability evaluation of distribution systems with nonexponential down times," *IEEE Transactions on Power Systems*, vol. 12, pp. 579–584, May 1997.

[26] E. Zio and L. Golea, "Analyzing the topological, electrical and reliability characteristics of a power transmission system for identifying its critical elements," *Reliability Engineering & System Safety*, vol. 101, pp. 67 – 74, May 2012.

[27] R. Fricks and K. Trivedi, "Importance analysis with Markov chains," in *Proc. of the Annual Reliability and Maintainability Symposium (RAMS)*, pp. 89–95, 2003.

[28] W. Wang, J. Loman, and P. Vassiliou, "Reliability importance of components in a complex system," in *Proc. of the Annual Reliability and Maintainability Symposium (RAMS)*, pp. 6–11, 2004.

[29] P. Crucitti, V. Latora, and M. Marchiori, "Locating critical lines in high-voltage electrical power grids," *Fluctuation and Noise Letters*, vol. 05, no. 02, pp. L201–L208, 2005.

[30] M. Rahim, I. Musirin, I. Abidin, and M. Othman, "Contingency based congestion management and cost minimization using bee colony optimization technique," in *Proc. of the IEEE International Conference on Power and Energy (PECon)*, pp. 891–896, 2010.

[31] S. H. Choo, S. Jang, J. Lee, J. Park, and J. Shin, "Approach on optimal generation and load control for enhancing voltage stability margin," in *Proc. of the Asia and Pacific Transmission Distribution Conference Exposition*, pp. 1–4, 2009.