Resilience of Electrical Power Delivery System in Response to Natural Disasters

Naresh Malla
EECS Department
South Dakota State University
Brookings, SD 57007
Email: naresh.malla@jacks.sdstate.edu

Shiva Poudel
EECS Department
Washington State University
Pullman, WA
Email: shiva.poudel@wsu.edu

Nava Raj Karki, Netra Gyawali
Department of Electrical Engineering
Central Campus, Pulchowk
Institute of Engineering
Tribhuvan University, Nepal
Email: nrkarki@gmail.com, netra@ioe.edu.np

***Abstract*—The electric power transmission and distribution system is a complex and critical part of the national infrastructure. The transmission lines may span hundreds of miles, may include multiple generators and substations, and many key facilities are unguarded. They may be located in vulnerable geographic location and have been attacked by natural disasters. Because of complex nature of todays power system, fault in any link may propagate to cause cascading failure and ultimately blackout. Thus it is necessary to study impact of natural disaster on electrical power systems for understanding the causes of the blackouts, explore ways to prepare and harden the grid, and increase the resilience of the power grid under such events. This study is conducted in order to assess the resilience of Electrical Power Delivery System (EPDS) of IEEE 14 bus system. The resilience is assessed through different techniques like cascading failure analysis for assessing the hazard, risk quantification and ranking for measuring the hazard, and islanding operation and detection for managing the hazard at the post disaster stage. Cascading failure analysis is performed for standard IEEE 14 bus system to determine the optimum value of system tolerance. Similarly, risk quantification criterion is applied to IEEE 14 bus system to determine the line which is most critical to natural disasters taking probability and severity into account. Finally, islanding operation and detection technique is employed to ensure survivability of IEEE 14 bus system even with limited operation.**

***Index Terms*—Electrical power delivery system (EPDS), resilience, cascading failure analysis, risk ranking, islanding operation.**

I. Introduction

The electric power transmission and distribution systems are the wires and associated equipment that carries power from central generators to end users. Such systems provide almost all of the electricity that is essential for the operation of the economy and for human well-being. The system is inherently vulnerable because transmission and distribution lines may span hundreds of miles, and many key components are unprotected. They also are difficult to protect and have been attacked by natural disasters. Therefore, it is important to think about what can be done to make them less vulnerable to attack, how power can be rapidly restored if an attack occurs, and how important services can be sustained while the power is out. The National Research Council (NRC) released a report in 2012 [1] that analyzed the vulnerability of the electric grid to terrorist attacks and measures to reduce that vulnerability. This works suggest that standardized design for substation transformer, improved instrumentation and controls over power flow on the grid can reduce outages. Literature [2] proposes a novel distribution system operational approach by forming multiple microgrids energized by diesel generation (DG) from the radial distribution system in real-time operations to restore critical loads from the power outage. A resilience-oriented service restoration method using microgrids to restore critical load after natural disasters is proposed in [3].

Many disasters like earthquake, thunderbolts etc. are inevitable in many part of the world. If any of these disasters hit the crucial part of transmission or distribution system, it could deny large regions of the country assess to bulk system power for weeks or even months. An event of this magnitude and duration could lead to turmoil, widespread public fear, and an image of helplessness. Electric systems are not designed to withstand or quickly recover from damage inflicted simultaneously on multiple components. Many power cables, mainly lower voltage lines, were cut by the shaking of the ground and failure of supporting poles. Since electricity is the most important lifeline facility, emergency efforts will be focused on their recovery by the management of Electricity Authority. The recovery of electric power will provide the suffering people with enhanced ability to promote rehabilitation, rescue/relief and recovery activities.

In recent years, United States have seen many blackouts due to natural disasters such as the 2005 Hurricane Katrina blackouts, and 2012 Hurricane Sandy blackouts. Between 2003 and 2012, roughly 679 power outages, each affecting at least 50,000 customers, occurred due to weather events in the U.S. Wang et al. [4] describes 933 events causing outages from the years 1984 to 2006. In Brazil, a cyclonic supercell thunderstorm developed in the countryside of the state, which stroke the outskirts of the city of Indaiatuba on 24 May 2005, producing a significant tornado collapsing nine 765 kV tower [5]. In Nepal, the devastating earthquake of April 25, 2015 and the series of aftershocks that followed the main shake have damaged around 14 hydropower plants across the country, resulting to loss of 150 MW of electricity from country's power grid. It damaged 14 existing hydropower dams, including the 45-megawatt Upper Bhotekoshi Hydropower Project. Nations power grid lost more than 30

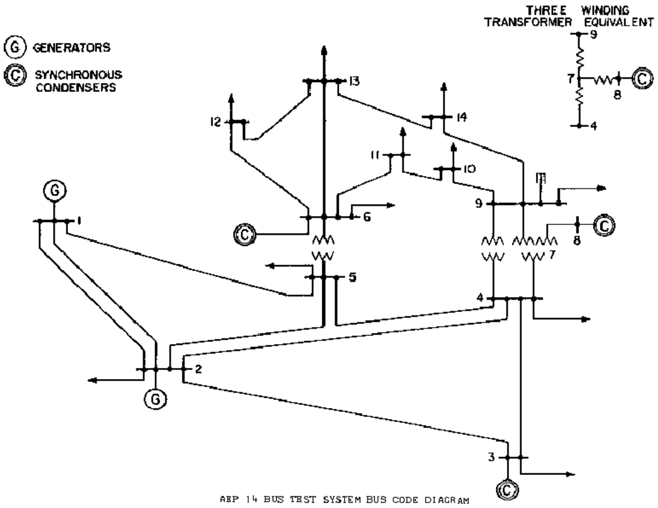

Fig. 1. Standard diagram for IEEE 14 bus system used as benchmark for study.

percent of generating capacity. Cracks also opened in the dam of the Kulekhani Hydropower Project. 10-megawatt Sunkoshi Hydropower Project, sustained serious damage for the second year in a row [6].

All of aforementioned literature motivates us to perform research on resilience of electric power grid. The resilience of the power grid is assessed in this research by using methods for assessing the hazard, measuring the hazard and managing it at post disaster stage. The hazard is assessed through cascading failure analysis. Cascading failure analysis is performed for standard IEEE 14 bus system as shown in Fig. 1 to determine the optimum value of system tolerance. Risk quantification and ranking technique [7] is used for measuring the hazard, and islanding operation and detection technique using residual vector method [8] is used for managing the hazard at the post disaster stage. Similarly, risk quantification criterion is applied to the IEEE 14 bus system to determine the line which is most critical to natural disasters taking probability and severity into account. Finally, islanding operation and detection technique is employed to ensure survivability even with limited operation for IEEE 14 bus system.

The rest of the section is organized as follows. Section II describes the methodology adopted for assessing, measuring and managing the hazard, and Section III describes simulation results. Section IV concludes the paper.

II. Methodology

1) assessing the Hazard: Cascading Failure Analysis
2) Measure Hazard: Risk Quantification
3) Manage Hazard: Operation of Power System during and at post-disaster condition (Island identification and detection technique)

A. Cascading Failure

The model of power grid and cascading failure will be introduced in this subsection, which will provide the electrical feature for comprehensive analysis. In order to present the power grid as a topological network, there are a few assumptions to be specified. First, a substation in the power grid cascading model is referred to as a node, regardless of its type as a generator, a load or simply a pass-through transmission substation; also, a transmission line which connects one substation at each end will be regarded as a branch in the network. Hence this helps to reduce the computational cost significantly while analyzing power grid [9]. Determining the most vulnerable components (e.g., buses or generators) is critically important for power grid defense. Previous work on cascading failures of high level power grid structure of Texas, USA in [9] have suggested that load of a particular node (substation) is related to the connectivity with/of its immediate neighbors [10]. This means that means that a node connecting to more neighbors, or whose direct neighbors have greater connectivity will be likely to take greater portion of load in the power delivery. The load of a node is defined as the product of its degree and the summation of the degree of all its neighbors. Degree of a particular node is defined as the number of neighboring nodes it is connected to. If Deg (v) is the degree of a particular node, the initial load, $L(v)$ is defined by:

$$L(v) = Deg(v) * \sum Deg(n), \quad n \in Nbr(v) \tag{1}$$

where Nbr (v) is the set of neighboring nodes of a particular node v. When a victim node is attacked or blacked out by cascading failure, its load will be proportionally redistributed to its neighbors according to:

$$L^{'}\left(n\right) = \frac{L\left(n\right)}{\sum L\left(n\right)} L\left(v\right), \; n \in Nbr(v) \tag{2}$$

This may lead to a new situation that these neighboring nodes will exceed their capacity and thus result in new failure. If the load lost that is to be reabsorbed is large, the failure propagation will continue and spread over the network and it continues until all the nodes are compromised which is referred as cascading failure in literatures [9], [10], [11]. Following [12], we define capacity $C(v)$ of each node which is directly proportional to its initial load L(v) that it carries in a healthy network as,

$$C\left(v\right) =\propto L\left(v\right), \quad v \in n \tag{3}$$

where, α is the system tolerance. Higher value of α means higher capability of the node to resist perturbations [11]. Affected by failure occurred elsewhere, some active nodes can be heavily overloaded and fail to operate as previous. So, considering a non-recoverable scenario, when a node is overloaded to a certain degree, it will be regarded as fatally overloaded and disconnected from the network. Then, all the branches that directly linked to it will also be cut off. The threshold of overloading ratio when a node fails is referred to as the system tolerance. As long as new fatally overloaded nodes emerge in the grid, the failure propagation will continue and eventually it will lead to a blackout. If the initial victims are properly selected, the natural disaster will be able to create a large scale or fast propagating blackout in the power system. When a number of nodes are failed, the concept of ”round” can be used to help describing the progress of failure cascading. The first set of victims consists of the failed nodes at first round. Then the nodes knocked down by the failure of initial victims directly will be regarded as the victims of second round, so on. In this way, failed nodes at different rounds in a cascading process form a tree-like structure. In this structure a node may have more than one parent if it is affected by multiple nodes failure at the same time. The load and status of each node is only updated once at each round, which means the nodes failed in the same round will not have instant effect on others. Instead, the failure of all nodes of last round will simultaneously affect the remaining active nodes in next round. At this moment, interest is in identifying the most critical components in the grid network from the cascading failure perspective. So a new metric, percentage of failure (PoF), is investigated to evaluate the damage caused by the failure of any grid components. Percentage of failure in the power grid with respect to system tolerance, denoted as POF, as the assessment metric is given by:

$$POF = \frac{N_f}{N} \tag{4}$$

where N_f is the number of failed components and N is the total number of components in a given grid. For each multi-victim attack, the value of PoF is measured after the cascading failure stops at the final stabilized state. High value of PoF indicates that the initial victims have resulted in a larger blackout with more component failed consequently after the initial attack; while with less PoF indicates a faster failure propagation with fewer intermediate process and requires a quicker decision to limit its impact at an early stage. By using this measurement, illustration can be made for the effectiveness of the proposed approach using the cascading failure model described above and highlight the critical components in the power grid in multi-victim attack scenarios [9].

B. Risk Quantification

Risk is defined as the probability of loss or damage to human beings, equipment, or assets [13]. Probabilistic risk is usually quantified in indices. Loss of load probability (LOLP) is the most common probabilistic reliability index in power system planning. However, this index reflects only the likelihood not severity. Other probabilistic indices such as the expected unserved energy (EUE), which represents the expected value of total energy not supplied during the study period, do capture the likelihood and severity, but the severity measure includes only load interruption [13], [14]. The index used in case of power system contingency analysis should reflect the composite nature of the likelihood of the outage and the severity associated with it. The latter includes deviations from acceptable thermal loading of transmission lines and transformers, or admissible bus voltage bounds, or from voltage stability or even transient stability in some cases. We employ the risk quantification ranking approach that accounts for both the severity and likelihood of the underlying system contingencies. We apply this technique to IEEE 14 bus system as shown in Fig. 1. The 14 bus system consists of 14 buses, 2 generators, 3 synchronous compensators, 11 loads, 17 transmission lines, and three transformers. Risk based security assessment (RBSA) is a relatively new approach that takes into consideration the uncertainty introduced by an actual power system operating condition as well as the severity of security violation should a contingency occur. The risk index developed through RBSA can quantitatively capture the probability of occurrence of each possible contingency that may cause security violation and the impact of the event. There are two important attributes in risk assessment, namely event likelihood, $Pr(E_i)$ and impact, $Sev(E_i, S)$. The ranked contingency values can be calculated using a combination of voltage risk index and transmission line risk index. An appropriate, quantitative risk index that captures the system exposure to failures as well as the expected severity of the contingency is given as:

$$Risk\left(S\right) = \sum_i \left(Pr\left(E_i\right) * Sev\left(E_i, S\right)\right) \tag{5}$$

where,

S: Loading condition

E_i=ith contingency (event)

$Pr\left(E_i\right)$=Probability of the occurance of the i^{th} contingency

Sev(E_i,S)=Severity of the i^{th} contingency occurring in S loading condition

The severity can be determined by analyzing system failure states and then assessing the consequences. The analysis can be related with the connectivity identification of a network configuration or the power balance [15]. The ranked contingency values can be calculated using a combination of voltage risk index and transmission line risk index which are described below.

1) Voltage Risk Index: The risk is associated with bus failure for this risk index. This is usually related to outage of the generator connected to a bus. The probability (Pr) of a generator failure (E_i) is calculated as follow with the assumption to be an exponentially distributed function.

$$\Pr\left(E_i\right) \; = \lambda e^{-\lambda t} \tag{6}$$

where, λ = forced outage rate of the connected generator or line. The severity function is calculated for each bus as follows:

$$VoltSev\left(Vj\right) = \begin{cases} \frac{0.94-|V_j|}{0.94}, |V_j| < 0.94 \\ 0,\ 0.94 < |V_j| < 1.06 \\ \frac{|V_j|-1.06}{1.06}, |V_j| > 1.06 \end{cases} \tag{7}$$

where V_j is the voltage at the respective bus j. The voltage limits are set to be 0.94 pu and 1.06 pu for the lower and upper limits respectively. There is no limit violation when the voltage is within this range.

2) Line Risk Index: For overload, the severity associated with the line is defined for each circuit specifically. This applies for both transmission lines and transformers. The line flow is denoted in percentage of rating (PR) in each circuit. The transmission line severity function is defined as follow:

$$LineSev\left(PR_k\right) = \begin{cases} \quad PR_k - 1.0, & PR_k \geq 1.0 \\ 0 & , \; PR_k < 1.0 \end{cases} \tag{8}$$

where, PR_k is the post-contingency percentage of rating (PR) corresponding to each overload. If there is no overload, then that particular line contingency do not pose critical limit violation in post-contingency system operation. The probability of the outage is considered here as the yearly outage rate representation of the transmission line.

3) RCR Calculation: The risk-based contingency ranking (RCR) metric sums up the risk attached to line contingency as well as bus contingency into a single quantifiable metric as:

$$RCR_j^{bus} = \sum_j \Pr\left(B_j\right) \; \times VoltSev\left(V_j\right) \tag{9}$$

$$RCR_k^{line} = \sum_k \Pr\left(L_k\right) \; \times LineSev\left(PR_k\right) \tag{10}$$

$$RCR = D \times RCR^{bus} + RCR^{line} \tag{11}$$

where,

Pr(B_j) : Probability of the occurrence of the j^{th}generation contingency

Pr(L_k) : Probability of occurrence of the k^{th} line contingency

D : Branch-node incidence matrix

The proposed RCR metric takes into accord both overload limit violations and voltage limit violations, due to line contingencies as well as generator contingencies. RCR metric combines the outages smoothly without the need to use weights, that are commonly assigned arbitrarily [7].

C. Operation of Power System during and at post-disaster condition

When disaster strikes power system components, it may: collapse, survive or run with limited operation. Among these, limited operation of power systems operating as several electrical islands is considered created as a result of large disturbances brought by disasters such as storms or hurricanes. It is thus of great importance to detect and identify these islands in order to capture the actual network model for further security analysis, emergency control and restoration. Given the recent proliferation of distributed power sources in power systems, a large number of these islands may still operate in the so called restorative state avoiding a complete system-wide blackout [16]. In power systems state estimator complete received data from the SCADA system. Power system state estimation is not required, if the received data from SCADA are adequate and correct. Power system state estimation with conventional and accurate method, Weighted Linear Least (WLS), is performed in two steps. In the first stage, the observability of system is done and then state estimation is carried out. Largest residual test is used in [17], [18] for identification of single and non-interacting multiple bad data with the help of Phasor measurement units (PMUs). For incorporating PMUs, the measurement function and its Jacobian have to be augmented by the phasor measurements. The details for this can be found in [19]. Since, a line outage can be treated as a virtual parameter error, whose admittance becomes zero, an existing parameter error identification algorithm is reviewed. Considering, parameters errors, the weighted least square (WLS) state estimation problem can be formulated as the following optimization problem:

$$Min : J\left(x\right) = r^T R^{-1} r \tag{12}$$

subjected to: $r = z - h(x)$ where,

r = measurement residual vector;

z = measurement vector

h(x)=nonlinear function of system state and parameters related to measurements;

x=system state vector: voltage magnitudes and angles.

R= Measurement Error vector.

The method for solving this state estimation problem is described in [20]. The algorithm for largest residual test is given as follows:

Algorithm 1 Algorithm for largest residual test [17]

```
1: Run WLS state estimation. In this step, all the measurement values obtained are the steady state values after system splitting, but the network model is still the same one before splitting.
2: Compute the elements of the measurement residual vector:
       $r = z - h$          (13)
   where, $z$=state vector $h$=nonlinear function of system state and parameters related to measurements.
3: Find $k$ such that $r_k$ is the largest among all $r_i$, $i = 1, , m$.
4: If $r_k > c$, then the $k^{th}$ measurement will be suspected as bad data.
5: Else stop, no bad data will be suspected. Here, $c$ is a chosen identification threshold, e.g. 0.1.
```

III. Simulation and Evaluation

A. Cascading Failure

The IEEE-14 bus system was studied for analyzing the bus failure due to disaster and how the cascading failure occurs. A simulator was built in MATLAB 2011b environment for simulating load redistribution process. Attack on nodes with the highest load is a common attack strategy and is based on the fact that the failure of a node with the largest value of load causes significant amount of load to be redistributed among its neighbors. The optimal strategy in this attack is to select the desired number of victim nodes in descending order of loads and to remove them from the network. In this model, load of a particular node is calculated using Eq. (1) described in

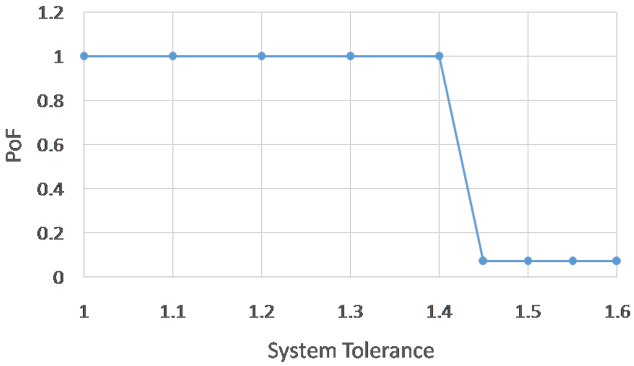

Fig. 2. Percentage of failure Vs System Tolerance for IEEE 14 bus system.

TABLE I
CASCADING FAILURE ANALYSIS FOR SYSTEM TOLERANCE=1.

Bus no.	L(v)	Capacity	1st attack	2nd	3rd	4th
1	16	16	16	43.84	0	0
2	52	52	73.25	0	0	0
3	18	18	25.36	0	0	0
4	85	85	0	0	0	0
5	60	60	84.52	0	0	0
6	44	44	44	76.21	0	0
7	30	30	42.26	0	0	0
8	3	3	3	4.8	0	0
9	48	48	67.62	0	0	0
10	12	12	12	31	0	0
11	12	12	12	12	61.29	0
12	14	14	14	14	35.34	0
13	24	24	24	24	96.75	0
14	14	14	14	36.17	0	0

methodology. Based on the loading information of all nodes, we initiated an attack on power system benchmark from load-based approach for simulating attack due to disaster. For traditional load based strategy, we sorted the nodes according to their initial load and found the most loaded ones to form the initial victim set as shown in Table I. In IEEE-14 bus system, it can be seen from Table I that node 4 is the most loaded one. In order to study the cascading failure process due to natural disaster, we knocked down the initial node in the benchmark system. This causes the redistribution of load in the remaining nodes according to Eq. (2) and it can be observed from Table I that some of the nodes are overloaded beyond their capacities. Next these overloaded nodes are also knocked down. This process was repeated several times until the system achieved final steady state. Finally, the number of survived components in steady state was evaluated and PoF was calculated using Eq. (4). Then, we increased the system tolerance and obtained the graph as shown in Fig. 2.

B. Risk Ranking

The ranking is carried out based on the severity (not the number of violations). The probability of outages is calculated using Eq. (6), based on the outage rates of generators and lines as tabulated in [7]. The RCR metric is calculated using Eq. (9) - (11). The list of ranked contingencies is given in detail in Table II.

TABLE II
RCR METRIC VALUES AND CONTINGENCY RANKING FOR IEEE 14 BUS SYSTEM

From Bus	To Bus	RCR Metric	Rank
1	2	0.178	1
1	5	0.0177	5
2	3	0.1663	2
2	4	0.0054	8
2	5	0.0126	6
3	4	0.0054	8
4	5	0.0438	4
4	7	0.0055	7
4	9	0.0054	8
5	6	0.0731	3
6	11	0.0054	8
6	12	0.0054	8
6	13	0.0054	8
7	8	0.004	9
7	9	0.0055	7
9	10	0.0055	7
9	14	0.0055	7
10	11	0.0054	8
12	13	0.0054	8

Results demonstrate that the most critical lines, in the top of the ranked contingency list, are 1-2, 2-3, 5-6, and 4-5. The results are not much different from those listed in [7], using the deterministic-based ranking. However, since the proposed RCR metric incorporates the probabilities of generator outage and line outage, line 1-2 is identified as the most critical contingency. This is due to the comparatively high outage rate of that line. In addition, it connects between two generator buses; of high outage rates as well. Similar argument applies, to a less extent though, to line 2-3.

C. Operation of Power System during and at post-disaster condition (Island identification and detection technique)

This method was implemented using the IEEE 14 bus test system. The system was randomly separated into two isolated islands due to a disaster [16]. Corresponding disconnected branches are B5-6, B4-9 and B7-9. The system was observable under conventional measurements as well as two PMUs at buses 1 and 6. Having at least one PMU per electrical island facilitates the process of solving the parameter error identification problem. As described in previous Methodology section, disconnected lines are identified one at a time until there are no suspect lines left by calculating the residual matrix using MATLAB which is given in Table III-C. It was found that branches, B5-6, B4-9 and B7-9 whose measurement numbers are 25, 22 and 39 respectively, have residual value greater than the threshold of 0.1. Table IV shows the highest value of residual matrix for these cases in Table III-C which is greater than threshold. Thus, bad data or disconnected line was identified using this method.

IV. CONCLUSION

This research was performed to study impact of natural disaster on electrical power systems for understanding the

TABLE III
RESIDUAL MATRIX VECTOR FOR NORMAL AS WELL AS LINE OUTAGE CONDITIONS

Measurement No.	Normal	5-6 outage	4-9 outage	7-9 outage
1	0.0533	0.0534	0.0533	0.088
2	-0.0031	-0.0031	-0.0031	-0.0041
3	0.001	0.0009	0.001	-0.0014
4	-0.0001	-0.0001	-0.0001	0.103
5	-0.0001	-0.0001	-0.0001	0.1049
6	-0.0002	0	-0.0002	-0.0002
7	-0.0006	0	-0.0006	-0.0007
8	0	0	0	0
9	0	0	0	0
10	0.0031	0.0031	0.0031	-0.0054
11	0.0095	0.0095	0.0095	0.0029
12	-0.0047	-0.0047	-0.0047	0.0502
13	-0.0044	-0.0044	-0.0044	0.0473
14	-0.0001	0	-0.0002	0
15	-0.0004	0	-0.0005	-0.0001
16	-0.0001	-0.0001	-0.0001	-0.0001
17	0	0	0	0
18	-0.0023	-0.0023	-0.0023	-0.0018
19	-0.0008	-0.0008	-0.0008	-0.0003
20	-0.0018	-0.0018	-0.0018	-0.0041
21	0.0003	0.0002	0.0004	0.0628
22	0.0004	0.0003	0.1546	0.0007
23	-0.0012	-0.0012	-0.0012	-0.0032
24	0	0	0	0.0002
25	-0.0002	0.4589	-0.0001	-0.0003
26	0	0	0	0
27	0.0001	0	0.0002	0.2707
28	0.0007	0	0.0007	0.0008
29	0	0	0	0
30	0.0018	0.0018	0.0018	-0.004
31	0.0103	0.0103	0.0103	0.0069
32	0.0041	0.0041	0.0041	-0.0033
33	-0.0026	-0.0028	-0.0027	0.0334
34	-0.0005	-0.0006	-0.0264	0.0005
35	0.0057	0.0057	0.0057	-0.0006
36	-0.0009	-0.0009	-0.0008	-0.0007
37	-0.0004	-0.2084	-0.0004	-0.0002
38	0	0	0	0
39	0.0033	0.0031	0.0032	0.148
40	0.0005	0	0.0006	0.0001
41	0.0001	0.0001	0.0001	0.0001

TABLE IV
ISLANDS IDENTIFICATION IN IEEE 14-BUS SYSTEM

Iteration Number	Parameter	r_k (max)	Outage line identified
1	R5-6=X5-6=Infinite	0.4589	6-May
2	R4-9=X4-9=Infinite	0.155	9-Apr
3	R7-9=X7-9=Infinite	0.148	9-Jul
4	Default	0.0533	None

causes of the blackouts, explore ways to prepare and harden the grid, and increase the resilience of the power grid under such events. This study was conducted in order to assess the resilience of Electrical Power Delivery System (EPDS) of IEEE 14 bus system. The resilience was assessed through different techniques like cascading failure analysis for assessing the hazard, risk quantification and ranking for measuring the hazard, and islanding operation and detection for managing the hazard at the post disaster stage. Cascading failure analysis was performed for standard IEEE 14 bus system to determine the optimum value of system tolerance. Similarly, risk quantification criterion was applied to IEEE 14 bus system to determine the line which is most critical to natural disasters taking probability and severity into account. Finally, islanding operation and detection technique was employed to ensure survivability of IEEE 14 bus system even with limited operation. Line 1-2 is found to be most critical to natural disasters with the highest risk ranking (measuring the hazard). Increasing the system tolerance above 1.45 would prevent cascading failure (assessing the hazard). Outage of lines 5-6, 4-9 and 7-9 would cause islanding operation, which could be detected by residual vector method (managing the hazard at post disaster condition). These tools can be used in any power system for assessing, measuring and managing hazard in case of natural disaster to identify the shortcomings and make the system resilient against such disasters.

REFERENCES

[1] N. R. Council *et al.*, *Terrorism and the electric power delivery system*. National Academies Press, 2012.

[2] C. Chen, J. Wang, F. Qiu, and D. Zhao, "Resilient distribution system by microgrids formation after natural disasters," *IEEE Transactions on smart grid*, vol. 7, no. 2, pp. 958–966, 2016.

[3] H. Gao, Y. Chen, Y. Xu, and C.-C. Liu, "Resilience-oriented critical load restoration using microgrids in distribution systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2837–2848, 2016.

[4] Y. Wang, C. Chen, J. Wang, and R. Baldick, "Research on resilience of power systems under natural disasters–A review," *IEEE Transactions on Power Systems*, vol. 31, no. 2, pp. 1604–1613, 2016.

[5] P. Gomes and N. Martines, "Resilience issues for the brazilian interconnected power system," 2014. [Online]. Available: http://www.eps.ee.kth.se/personal/vanfretti/events/stint-capes-resiliency-2015/10_Nelson.pdf

[6] R. Pangeni, "My republica - earthquake damages over dozen hydropower projects," 2017. [Online]. Available: http://admin.myrepublica.com/economy/story/20398/earthquake-damages-over-dozen-hydropower-projects.html

[7] W.-S. Tan and M. Shaaban, "Ranking of power system contingencies based on a risk quantification criterion," in *Research and Development (SCOReD), 2015 IEEE Student Conference on*. IEEE, 2015, pp. 356–361.

[8] A. Abur, "State estimation," 2014. [Online]. Available: https://pdfs.semanticscholar.org/6621/7381559f8bf0c9a003d42a49640a-add1718c.pdf

[9] J. Yan, Y. Zhu, H. He, and Y. Sun, "Multi-contingency cascading analysis of smart grid based on self-organizing map," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 646–656, 2013.

[10] S. Poudel, Z. Ni, X. Zhong, and H. He, "Comparative studies of power grid security with network connectivity and power flow information using unsupervised learning," in *Neural Networks (IJCNN), 2016 International Joint Conference on*. IEEE, 2016, pp. 2730–2737.

[11] S. Poudel, Z. Ni, T. M. Hansen, and R. Tonkoski, "Cascading failures and transient stability experiment analysis in power grid security," in *Innovative Smart Grid Technologies Conference (ISGT), 2016 IEEE Power & Energy Society*. IEEE, 2016, pp. 1–5.

[12] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *nature*, vol. 406, no. 6794, pp. 378–382, 2000.

[13] W. Li, *Risk assessment of power systems: models, methods, and applications*. John Wiley & Sons, 2014.

[14] M. Shaaban, "Risk-based security assessment in smart power grids," in *Innovative Smart Grid Technologies-Middle East (ISGT Middle East), 2011 IEEE PES Conference on*. IEEE, 2011, pp. 1–5.

[15] M. Ni, J. D. McCalley, V. Vittal, and T. Tayyib, "Online risk-based security assessment," *IEEE Transactions on Power Systems*, vol. 18, no. 1, pp. 258–265, 2003.

[16] L. Zhang and A. Abur, "Post disturbance island identification via state estimation," in *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*. IEEE, 2012, pp. 1–5.

[17] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC press, 2004.

[18] J. Zhu and A. Abur, "Identification of network parameter errors," *IEEE Transactions on Power Systems*, vol. 21, no. 2, pp. 586–592, 2006.

[19] ——, "Improvements in network parameter error identification via synchronized phasors," *IEEE Transactions on Power Systems*, vol. 25, no. 1, pp. 44–50, 2010.

[20] S. M. Mahaei and M. R. Navayi, "Power system state estimation with weighted linear least square," *International Journal of Electrical and Computer Engineering*, vol. 4, no. 2, p. 169, 2014.