Journal of Operation and Automation in Power Engineering

Vol. 13, No. 2, Apr. 2025, Pages: 165-173

http://joape.uma.ac.ir

Research Paper

Static Security Assessment of Integrated Power Systems with Wind Farms Using Complex Network Theory

Farshad Babaei[1], *Amin Safari*[1,*], *Javad Salehi*[1], *and Hossein Shayeghi*[2]

[1] *Department of Electrical Engineering, Azarbaijan Shahid Madani University, Tabriz, Iran.*
[2] *Department of Electrical Engineering, University of Mohaghegh Ardabili, Ardabil, Iran.*

Abstract— *Although the presence of clean energy resources in power systems is required to reduce greenhouse gas emissions, system security faces severe challenges due to its increased intelligence and expansion, as well as the high penetration of renewable energy resources. According to new operating policies, power systems should withstand subsequent single contingencies. Also, the effect of electrical and structural characteristics must be considered in power system security assessment. Thus, this paper introduces a comprehensive risk-based approach that quantifies the impact of contingency-induced variation in topology by using complex network theory metrics. Then, it identifies elements that surpass security limitations and eliminates them to execute cascading outage analysis via AC power flow. Lastly, wind power uncertainty and contingency probability are multiplied by the linear combination of electrical and structural consequences, and security status is assigned to each contingency based on its risk value. Additionally, simulations are carried out on modified 118 and 300 bus IEEE systems, and the extensive results are utilized to demonstrate the effectiveness of the proposed methodology.*

Keywords—Cascading failure, complex network theory, security assessment, risk index, wind farm.

1. Introduction

Lately, the global tendency toward environmentally sustainable power generation strategies has stoked the high penetration of renewable energy resources and the increasing complexity of the power system. On a broader scale, however, new knowledge of power system operation is necessary, and potential barriers come into being to the power system's stability and security. Hence, the future of the electricity industry will look very different thanks to the impact of climate change and other environmental issues. Due to recent blackouts [1], it can be understood that security analysis is critical in a modern power system. Static and dynamic security assessments are the two basic security assessment studies. The former examines the steady-state reaction of the power system when a contingency occurs. In contrast, the latter assesses the system variables before the contingency, immediately after, and during the transient period.

1.1. Literature review

This section begins with an overview of power system security assessment methods. Then, it examines the risk-based approaches in more detail. According to previous studies, it can be found that power system security is classified into three categories based on analysis methods: deterministic, probabilistic, and risk-based techniques. Many deterministic methods based on the N-1 criterion assess the power system's security under the predefined contingency list. In these cases, the power system is kept close to security margins to cope with the worst-case scenario [2]. However, the deterministic approach disregards the power system uncertainty and complexity in the operating mode. Probabilistic methods can offer a better idea of how safe a power system is because they consider the probability of contingency occurrence and the power system various uncertainties [3]. Also, a risk-based approach combines the consequences of the contingency and their probability for investigating power system security [4].

Today, power system security analysis under risky conditions is critical work. The power system vulnerability analysis has attracted the researcher's attention as a crucial piece of security assessment. Several researchers are trying to identify indexes to address the transmission line vulnerability, while others are attempting to improve the security of power system infrastructure against contingencies. The steady-state risk assessment of the power system using the Monte Carlo method has been addressed in Ref. [5]. Despite introducing security regions and uncertain system topology variation, the proposed algorithm is complicated and time-consuming. A technique to estimate the risk of line overloading is described in [6]. In Ref. [7], a risk-constrained stochastic scheduling model is proposed using the latent scheduling capacity of multiple energy systems. In [8], a framework for transient stability risk assessment considering the load level is presented. Ref. [9] undertakes a risk assessment of hybrid storage systems using an enhanced fuzzy synthetic evaluation method. The fuzzy approach has many advantages, like solving complex multi-factor and multi-level problems. However, its major drawback is that it disregards the unpredictability of the external environment. Ref. [10] models the likelihood and effect of wind uncertainties and line flow oscillation in the risk index and then quantifies power system security using it. One of the significant drawbacks of this method is the dynamic line rating. It imposes more uncertainty on the power system and may lead to additional operational losses due

Received: 06 Aug. 2023
Revised: 17 Nov. 2023
Accepted: 28 Nov. 2023
*Corresponding author:
E-mail: asafari1650@yahoo.com (A. Safari)
DOI: 10.22098/joape.2023.13644.2044

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.
Copyright © 2025 University of Mohaghegh Ardabili.

to the random nature of line ratings and wind power generation. A new security assessment of a modern power system with a high penetration of wind power generation is given in [11]. It uses sequential time simulation to develop risk-based security analysis and considers overload risk based on the continuous severity function. Despite the convenient implementation of sequential algorithms, they are impractical for large-scale systems due to their high execution time. The robust security assessment that measures the security level according to dynamic economic dispatching using the DC power flow is formulated as a bi-level optimization problem and is presented in Ref. [12]. The security assessment tools can be developed using artificial intelligence and machine learning techniques. These methods provide a qualitative and quantitative assessment of power system security. For instance, the interleaved index-based intelligent design has been applied to assess smart grid security in Ref. [13]. This index comprises the Lyapunov exponent section to track uncontrolled power flow increases and another to monitor line overload.

The power system security evaluation in [14] employs quicker indexing based on artificial neural networks. Although the neural network replaces conventional techniques to achieve the desired speed and accuracy, it faces significant problems, such as an extensive training process, complicated design procedures, and the need to be more accurate when some components are strongly correlated. Ref. [15] used a machine-learning-based security assessment to reduce the simulation burden caused by unpractical phenomena in real time. The researchers are motivated by the advances in complex network (CN) theory to analyze networks from a novel structural view regarding nodes and their connections. Finding the power system's weak points and analyzing the operational characteristics, which may be done with a CN theory, are helpful steps toward a technical analysis of the power system's performance. The CN theory can be employed to evaluate power system security by identifying the critical branches or buses [16]. From the CN theory perspective, many studies show that transmission network fault propagation can extend to non-adjacent branches and adjacent branches [17]. Because of the small-world properties, the branches may impact one another during a failure operation. Scale-free features [18] show that electrical networks are sensitive to planned attacks but robust to random attacks when crucial branches are removed from the networks to explore their corresponding loss of load. Power systems are particularly vulnerable to purposeful attack because they are scale-free, requiring the precise identification of important branches (or buses). Today, the statistical indices of the CN theory, like degree, betweenness and closeness, are used for risk-based security assessment [6–8]. Even though the comprehensive statistical indices take the physical characteristics of the power system into account, they are still skewed toward the structural vulnerability analysis of the electrical networks.

Consequently, applying the CN theory to analyze operational risk remains problematic and has been studied more thoroughly. Taking statistical graphs, such as cascading fault graphs [19, 20], risk graphs [21, 22], influence graphs [23], and interaction graphs [24, 25], besides structural and electrical characteristics, can be advantageous. The statistical graphs point out the propagation path of faults and the temporal correlations between branches. Numerous studies have observed that the power grid system adheres to the small-world model and have demonstrated the profound repercussions that can arise from a few critical nodes and lines in the overall design [26]. These findings underscore the significant consequences that can result from the power grid topology variation under severe attacks. Moreover, much literature has focused on developing algorithms to enhance the efficiency of complex networks within network theory [27, 28]. While several studies have examined the application of CN theory to the power grid, only a few have emphasized analyzing the potentially severe outcomes encountered by the power grid. Although many researchers have provided metrics based on the topological model, they should have paid more attention to the indicators corresponding to the power system operating mechanism. The shortcomings above led us to attempt to improve the ability of the power system to prevent the occurrence of widespread outages caused by single contingency and to achieve a practical security assessment approach.

1.2. Contributions

A significant portion of the studies in electrical engineering have been focused on power system security assessment. In contrast, only some have addressed both structural and electrical indices simultaneously. Our paper is motivated by the necessity for a risk-based security assessment to identify critical transmission lines in integrated power systems with wind farms. In summary, this paper's contributions can be stated as follows:

- Investigation of the impacts of RES penetration on power system security
- Presentation of a new risk index (based on structural and electrical indices) to identify the set of power system vulnerable lines
- Consideration of the probability of a line outage and its impact on the security assessment
- Classification of security status based on the proposed risk index.

Next, a general description of how contributions were achieved is explained. The Weibull distribution function examines the uncertainty associated with wind power generation. Also, a new probability concept is presented to estimate the transmission line outage. It incorporates transmission line tripping and unavailability concerning line ampacity and environmental parameters like sunshine intensity and ambient temperature. Then, the cascading outages resulting from the initial contingency are computed. The electrical risk index caused by the cascading outages is added to the structural risk index. Finally, the comprehensive risk index is computed, and the power system security status is defined according to the levels presented in Section 4.

1.3. Orgnization

The rest of the paper is provided as follows: Section 2 presents the CN-based power system indicators, and the security evaluation index is investigated in Section 3. The security assessment procedure and simulation results are shown in sections 4 and 5, respectively. Finally, the paper concludes in Section 6.

2. CN-BASED GRID MODEL INDICATORS

According to the CN theory, this section develops a power-weighted grid complex network model. It proposes indicators for evaluating the grid network's properties. CN theory assumes that any given network could be represented as G = (N,E) , where N and E are sets of nodes and edges, respectively. Hence, this paper considers the generator and load as CN nodes and transmission lines between nodes as its edges to develop a power system model based on CN theory and analyze its operation characteristics. As is known, an edge is created between two nodes whenever a physical line connects them. Also, an adjacency matrix is used to record the underlying relationship between the nodes, where the presence/absence of a connection relationship is shown by 1 and 0, respectively. Due to the edge direction in the directed network, the adjacency matrix is not necessarily symmetric. CN theory was used to develop grid network characteristics indicators based on the weighted model. In this model, edge weight is determined by line impedance. Thus, the shorter the distance, the greater the power.

2.1. Electrical and edge betweenness

With the traditional topological method, betweenness is calculated as the probability that a given node or edge is part of a randomly chosen geodesic path connecting any other pair of nodes. It is a more suitable tool for estimating the critical load on a specific network edge. One of the most influential segments of betweenness is network connectivity. The betweenness is a local metric to describe the centrality value and criticality of elements. It evaluates how significant an edge is in a network structure. The betweenness centrality is the ratio of the number of the shortest paths containing a line over the number of all the shortest paths. The larger this index is, the greater the number of the shortest paths traversing the edge and the higher the power flow stress. In this paper, betweenness centrality can be obtained as follows [29]:

$$B_l = \sum_{i}^{N} \sum_{j}^{N} \frac{\sigma_{ij}(l)}{\sigma_{ij}}. \tag{1}$$

Where, the number of the shortest path between i and j that passes through line l is represented by $\sigma_{ij}(l)$. An example of edge betweenness centrality is given in Fig. 1. According to the value of the individual betweenness centrality and the number of two-hop neighbours they are connected to, the logical neighbours are selected. Since all 2-hop neighbours can be reached through node 2, and the edge connecting nodes 1 and 2 has a higher EBC value than the edge connecting nodes 1 and 3, node 1 will decide to broadcast only to node 2.

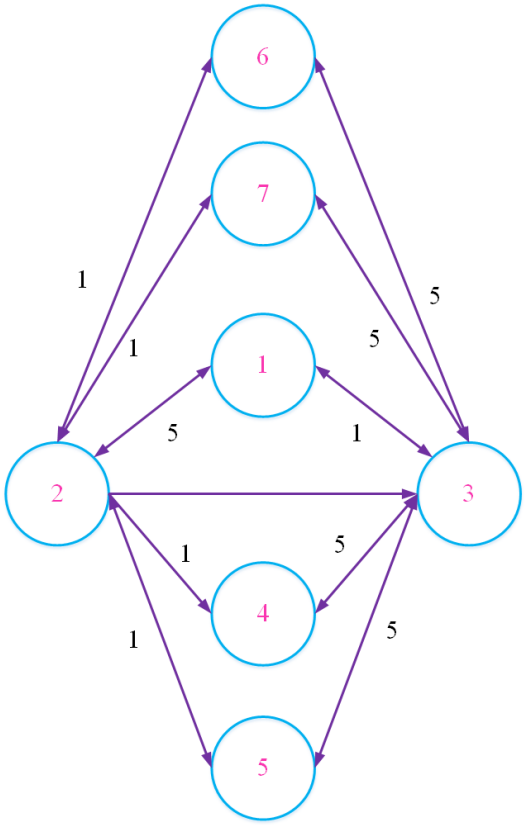

Fig. 1. Description of edge betweenness centrality.

2.2. Clustering coefficient

A network's aggregation is measured by the clustering coefficient, which shows how closely the network's nodes are connected. If it is assumed that the neighbour sets of node i are $N(f)$, and $|N(f)|$ equals k_i, then the clustering coefficient of node i can be expressed as the ratio of the number of edges E_i to the total number of potential edges [29].

$$C_i = \frac{2E_i}{k_i(k_i - 1)}. \tag{2}$$

The clustering coefficient is a critical measure for describing the network's structural properties. The average clustering coefficient C indicates the average of all node clustering coefficients, which is 0 when all nodes are isolated and 1 when all nodes are connected.

3. Security Evaluation Index

The power security metrics should support the predominance of complex network methodologies in structure analysis and account for the unique characteristics of power system engineering. For this purpose, two distinct aspects, operating status and network structure, are recommended for resolving power system security issues. This paper presents the power system structural security index to measure the impact of contingency occurrences.

3.1. Lost load

When random disturbances cause grid edges to become overloaded, the whole grid load will accordingly alter. The percentage of lost load, denoted by P_L, is calculated by dividing the removed load in the current operational state by the initial power system load.

$$P_L = \frac{\sum\limits_{j \in G_1} L_j}{\sum\limits_{j \in G_0} L_k}. \tag{3}$$

Where, set of healthy and failed load nodes are represented by G_0 and G_1, respectively. Also, L_j and L_k are the loads of of jth and kth nodes.

3.2. Lost generation capacity

During the cascading process, a portion of the network generation capacity (generator node) will be lost due to the expansion of the edge's failure and inability to transfer power to other nodes. In this paper, lost generation is defined as the ratio of forfeited generation in the current operational state to the total power system generation.

$$P_G = \frac{\sum\limits_{j \in H_1} P_j}{\sum\limits_{j \in H_0} P_k}. \tag{4}$$

Where, H_0 and H_1 reflect a set of the available and failed generator nodes, respectively. Also, P_j and P_k represent the power generation value at the jth and kth nodes.

3.3. Power system connectivity

Network connectivity indicates the network's ability to keep going and operating despite the unexpected loss of a power system component. In other words, the reliability and efficacy of complex networks are contingent upon their connectivity. It is defined as the ratio of the number of healthy nodes and edges in the power system to their total number.

$$Q_i = 1 - \frac{N_{f,i}}{N_t}. \tag{5}$$

Where, $N_{f,i}$ and N_t indicate the number of failed and total power system elements, respectively. When the survivability index reaches zero, the power system is at severe risk; whenever it leans towards 1, the grid will be in an appropriate state.

3.4. Power system vulnerability

The vulnerability index provides a numerical measure of how vulnerable a system or its components are. From a vulnerability perspective, a minor disturbance can result in disastrous consequences. In order to assess the grid's vulnerability, the network average clustering coefficient ratio is presented.

$$C = \frac{C_1}{C_0}. \tag{6}$$

Where, C_0 and C_1 reflect the network's average clustering coefficients before and after contingency.

3.5. Power system transmission efficiency

The analysis of only a few fundamental topological metrics can disclose only the structural characteristics of the sequential system. Hence, to assess how well a power system transmits energy, the following efficiency index can be used [30].

$$E_i = \frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{d_{ij}}. \tag{7}$$

According to Eq. (7), the transmission efficiency of a weighted network is the inverse of the shortest path between any two nodes. Assuming that there is no direct link between nodes i and j, it can be seen that $d_{ij} \to \infty$ at this point and that $(1/d_{ij}) \to 0$ after that. Therefore, we have assumed that topological efficiency corresponds to the power flow in a line. As a result of removing a line or node, the loss of transmission efficiency leads to a decline in average power. The network transmission efficiency reduction, E, is calculated as the ratio of current network transmission efficiency, E_i, to its initial value, E_0 .

$$E = \frac{E_i}{E_0}. \tag{8}$$

3.6. Wind power modeling

Here, the wind speed data is considered using the Weibull distribution and its probability density function formula is given as [31, 32].

$$f(v) = \frac{\gamma}{\alpha}(\frac{v}{\alpha})^{\gamma-1} \exp(-(\frac{v}{\alpha})^{\gamma})) \quad v > 0, \gamma > 0, \alpha > 1. \tag{9}$$

In Eq. (9), wind speed, shape and scale parameters are shown by v, γ and α, respectively. Although α is highly dependent on the wind farm location, we only consider a single value because this work regards the aggregated zonal wind power without taking wind farm size into account. Note that the AC power flow uses wind power generated with γ = 2 and α = 11 for non-correlated situations. Note that two main factors, line ampacity and environmental parameters like sunshine intensity, ambient temperature, etc., affect the temperature of the transmission line conductor. Here, weather-based transmission line loading and their unavailability index are used to calculate the line outage probability. According to the IEEE 738 standard, the steady-state heat balance equation is provided by [33]:

$$q_c + q_r = q_s + I^2 R_{Tc}. \tag{10}$$

where q_r and q_c are the radiative and convective heat losses while q_s, I and R_{Tc} are the solar heat gain, current flowing through the conductor and resistance at the specific temperature. Using Eqs. (11) to (13), the radiative and convective heat losses as well as solar heat gain are calculated as [34]:

$$q_s = \alpha_s Q_s \sin(\eta) d, \tag{11}$$

Table 1. Simulation parameters.

Parameters	Description	Value
α_s	Solar absorption rate	0.27
η	Angle bet line and light	30°
d	Conductor diameter	0.02 (m)
λ_f	Air thermal conductivity	0.024
ρ_f	Air density	1.225 (Kg/m3)
v_w	Wind speed	0-8 (m/s)
μ_f	Air viscous coefficient	1.81×10^{-5} Pa.s
ε_r	Line emissivity	0.9
σ	Stefan-Boltzmann constant	5.67×10^{-8}
R_{dc}	Resistance	$0.0738 \times 10^{-3}(\Omega/m)$
k	Temperature rise coefficient	$0.0039(\Omega/^{\circ}C)$

$$q_r = \pi d \varepsilon_r \sigma([T_c + 273]^4 - [T_\alpha + 273]^4), \tag{12}$$

$$q_c = 0.641 \pi \lambda_f (T_c - T_\alpha)(\frac{d \rho_f V_w}{\mu_f})^{0.471}. \tag{13}$$

The variables used in the correlations discussed above are listed in Table 1.

The rated current can be computed as follows if the line type and meteorological data are known:

$$I_{nom} = \sqrt{\frac{q_c + q_r - q_s}{R_{Tc}}}. \tag{14}$$

The conductor's internal charge carrier collision frequency increases along with its temperature rise. Thus, the lines' conductor resistance will increase as follows [34]:

$$I_{line} = \frac{U}{R_{dc}(1 + k\Delta T)}. \tag{15}$$

Hence, weather-based line tripping is calculated as:

$$P_{line\_trip,l} = \begin{cases} 1 - \exp(-10 \times (\frac{I_{line,l}}{I_{nom,l}} - 1)) \ , \\ I_{line} > I_{nom}. \end{cases} \tag{16}$$

On the other hand, the ratio of the number of hours a transmission line is out of service to the entire time the line is in use is defined as unavailability.

$$U_l = \frac{T_{out_l}}{T_{out_l} + T_{in_l}}. \tag{17}$$

Where, T_{out} and T_{in} represent the total time the line i is out of service and is in service, respectively. Finnaly, the combined line outage probability is given as:

$$f(l) = P(line\_trip_l \cap U_l) = P_{line\_trip_{,l}} \times U_l. \tag{18}$$

Typically, the probability and consequences of contingencies are multiplied to determine risk levels, while other variables, such as weighting, may also be considered. Due to the above assumptions, a comprehensive metric to evaluate the power system risk-based security is obtained as follows:

$$\begin{aligned} &Risk_l = P_l \times C_l, \\ &\text{where} \\ &\qquad P_l = f(l) \times f(v), \\ &C_l = (Q_l(P_{L,l} + P_{G,l})) + \beta((1 - E_l) + (1 - C_l)). \end{aligned} \tag{19}$$

The bigger $1 - E_l$ and $1 - C_l$ parameters provide a more significant threat to power system security. For this reason, the β coefficient is used to illustrate their importance in Eq. (19). Note that this coefficient is set to 10 here.

4. Security Assessment Procedure

Fig. 2 depicts the overall structure of the power system employed in this work. Conventional power plants and wind farms regulate the power flow. The power system must be stable to prevent the loss of a significant component in the case of a transmission system. Therefore, the line outage is considered to be a contingency.

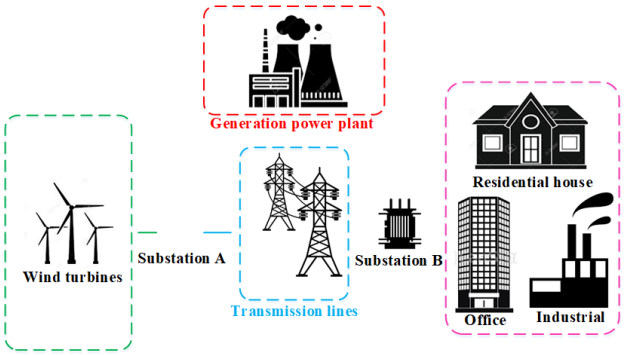

Fig. 2. Comprehensive structure of the power system.

The operating state and network structure are presented as two different aspects of resolving power system security issues, and their relationships are examined. Thus, it is emphasized that power security metrics should maintain the dominance of the complex network approach in structure analysis and consider the unique characteristics of power system engineering. In this paper, transmission efficiency and average clustering as complex network metrics are used to compute the risk level of line outages. Also, the cascading failure process is applied to quantify the effects of line outages in the power system. According to Fig. 3, the cascading failure procedure can be separated into three stages: the trigger, expansion, and collapse.

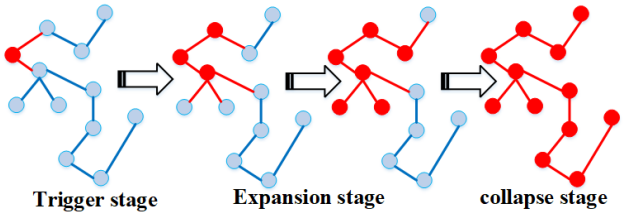

Fig. 3. Cascading failure procedure.

In summary, the power system security assessment procedure is broken down into the following steps:

Step1: Removing the ith branch (edge)

Step 2: Running power flow; if it is converged, go to the next step; if not, execute load shedding and resume power flow.

Step 3: Checking for line overload; if a line is overloaded, run the cascading failure analysis course.

Step 4: Calculating the grid security assessment index.

Step 5: Were all line outages evaluated? If not, return to step one; otherwise, proceed to the next step.

Step 6: Here, line outages are ranked, and the power system security status is finally defined based on this ranking.

The flowchart methodology of this paper is presented in Fig. 4. Classifying the security levels of the power system is essential to investigating its security state and improving it. Because grid security is affected by the power system's structure and its operating conditions, the security levels should be categorized according to these two factors. For this reason, the proposed risk index is selected. The power system is divided into four security levels using proposed risk index values.

Level 1: $Risk_l = 0$

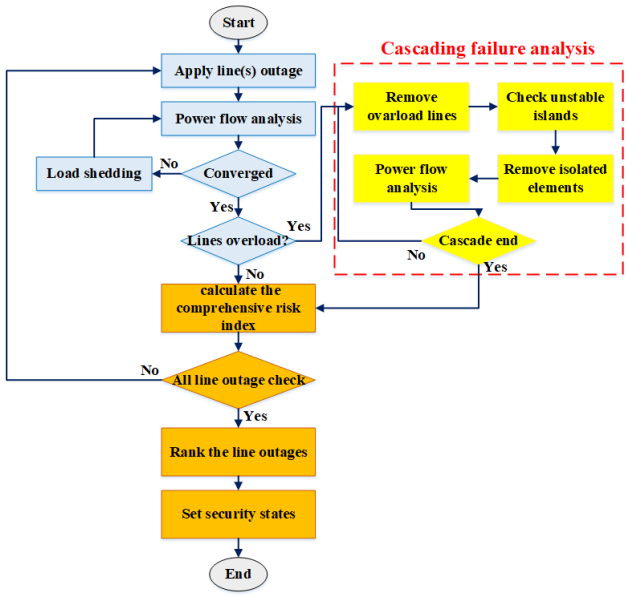

Fig. 4. Flowchart methodology for power system security assessment.

The grid security level is high for specified contingencies.

Level 2: $0 < Risk_l < 1$

Here, the grid security level is normal.

Level 3: $1 < Risk_l < 5$

In this case, the grid security level is low, and the overloaded lines lead to operational issues.

Level 4: $Risk_l > 5$

There is a high security risk, and the operators take immediate action to mitigate the significant security threat they face.

5. Simulation Results

The power system must resist the loss of a significant element in a transmission trip. Hence, a line outage is considered a contingency. In this section, the proposed method for risk-based security assessment is implemented on diverse standard networks, including IEEE 118, modified IEEE 118, and 300 bus systems. It should be noted that the power flow solution is computed using data from the cases in Matpower. Also, all algorithms are programmed in Matlab 2017a and executed on a computer with a Core i3 2.40 GHz CPU and 4 GB of memory.

5.1. Risk evaluation on IEEE 118-bus system

The IEEE 118-bus system illustrates a simplistic estimation of the power system in the Midwest of the United States. It has 19 generators, 35 condensers, 186 lines, and 91 loads [35]. Under normal operating conditions, the total generation capacity is 4377.4 MW and 1474.94 MVar, whereas the total load is 4242 MW and 1438 MVar. Here, the contingency set is first constructed. Then, the grid operating situation is measured by the power flow solution after the contingency. When power flow calculations do not converge, load shedding is performed in steps. When a line's maximum capacity is exceeded, it is removed from the power system, and this procedure continues until there are no more overloads. Finally, the consequences of line outages are evaluated by the electrical and structural indices mentioned above. The 138, 230, and 345 kV circuit outage data by average duration for 2015–2019, as well as their transformer data, are reported in Ref. [36]. The obtained risk indices are sorted for assessing the severity of line outages. The 20 contingencies with the highest ratings are shown in Table 2.

Based on the proposed risk index, transformer 5-8 is the most essential elements in the overall system. Also, in previous literature

Table 2. Risk of the line outages for IEEE 118 bus system.

Line	From bus	To bus	Risk
L8	8	5	3.088503
L36	30	17	3.081106
L21	15	17	2.993498
L38	26	30	2.540655
L96	38	65	1.454068
L51	38	37	1.351755
L69	48	49	1.129388
L68	45	49	1.129388
L83	51	58	1.062208
L129	82	83	0.914758
L107	68	69	0.906882
L7	8	9	0.849253
L81	50	57	0.779599
L9	9	10	0.727632
L40	29	31	0.676063
L66	42	49	0.658092
L37	8	30	0.603534
L54	30	38	0.455442
L62	45	46	0.445464
L33	25	27	0.404201

[37, 38], this branch has been identified as a contingency with the potential for starting and spreading cascading failures in the IEEE 118 bus system, leading to blackouts. Thus, the correctness of the obtained results is confirmed by past works. The generator at node 10 and the area of zone 1 with the highest load concentration are linked together primarily through this transformer. Transformers 5-8 and other grid branches going out at once cause cascade failures to start. In addition, the disconnection of transformers 5-8 causes lines 8–30 to become overloaded. The security risk index for all line outages in this system is illustrated in Fig. 5.

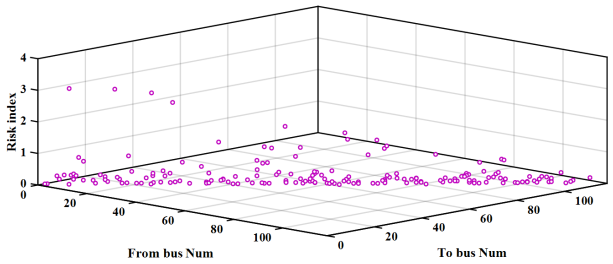

Fig. 5. Line outages risk for IEEE 118 bus system.

5.2. Risk evaluation on modified IEEE 118-bus system

Simulation is performed on the modified IEEE 118 bus system to investigate the effectiveness of the proposed security assessment method. For this goal, it has been constructed by adding 11 wind generators and 4 energy storage systems to the IEEE 118-bus system. Note that information on the installed capacity and location of wind generators and energy storage systems is provided in Ref. [39]. In this case, simulations are performed on the same calculation platform. Due to the results presented in Table 3, high penetration of wind power can lead to an increase in the degree of power system risk. Here are some of the contingencies with the highest risk level.

Also, the computed risk index for all line outages is illustrated in Fig. 6.

The risk-based security assessment process previously discussed is used to identify the critical branches in the modified 118 bus system. According to the proposed risk index, it has been determined that Lines 89–92 and Transformers 37–38 are the two components of the overall system that are of the highest importance. The failure of lines 89–92 has resulted in the disconnection of a generation capacity of 810 MW that was

Table 3. Risk of the line outages for the modified IEEE 118 bus system.

Line	From bus	To bus	Risk
L161	**89**	**92**	**20.62431**
L59	**38**	**37**	**19.96280**
L157	89	90	2.15620
L94	54	59	1.21720
L46	29	31	1.01920
L76	42	49	1.00960
L77	45	49	1.00960
L90	56	57	0.83460
L91	50	57	0.83460
L9	8	5	0.82757
L40	27	28	0.78500
L41	28	29	0.78500
L74	47	49	0.51340
L103	61	62	0.40860
L148	82	83	0.40480
L149	83	84	0.40480
L166	94	95	0.39840
L130	69	75	0.38980
L131	74	75	0.38980
L70	45	46	0.35960

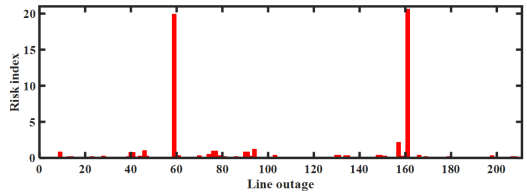

Fig. 6. Line outages risk for all branch of modified IEEE 118 bus system.

previously linked to buses 87 and 89. It is noted that generator failure leads to frequency instability and starts cascading failures that culminate in a power system blackout. Figs. 7 and 8 depict the out-of-service branch or node and the loss of load and generation, respectively. Fig. 9 illustrates the risk resulting from complex network indicators in the aforementioned system.

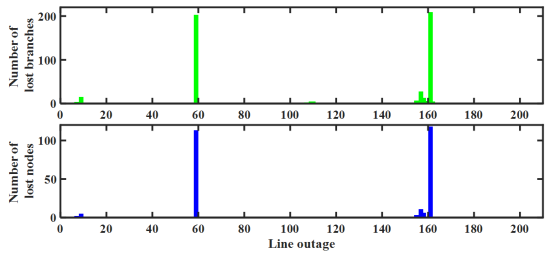

Fig. 7. Loss of branch and node for each line outage in modified IEEE 118 bus system.

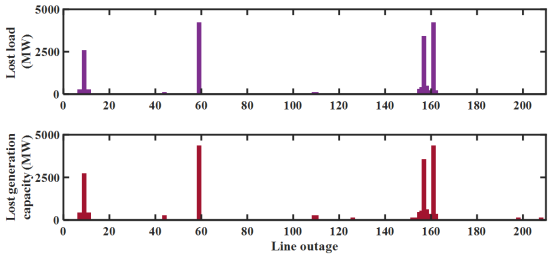

Fig. 8. Lost load and generation for each line outage in modified IEEE 118 bus system.

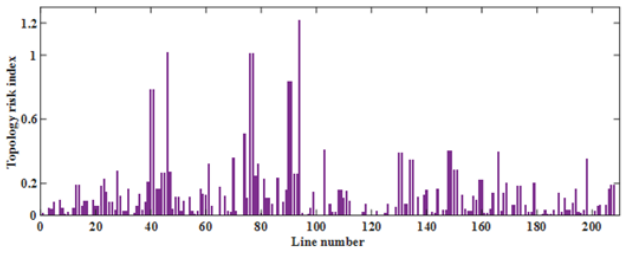

Fig. 9. Topology risk index for modified IEEE 118 bus system.

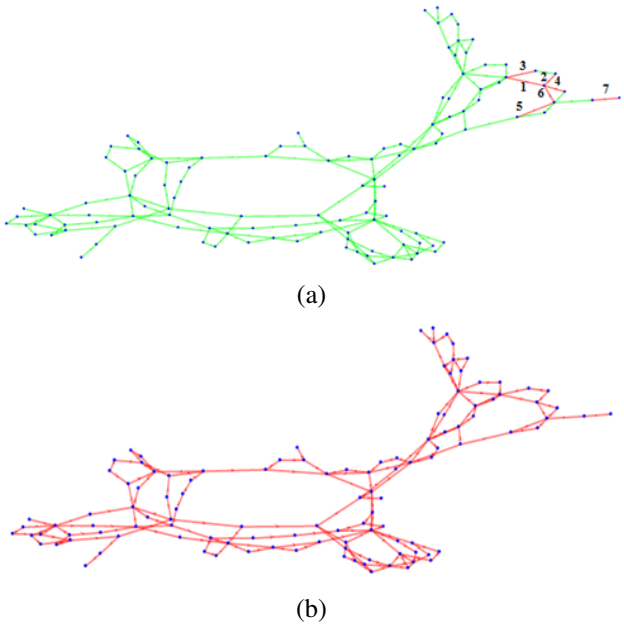

Fig. 10. a) Cascading failure stages, b) Blackouts caused by the line outage 161.

In the modified IEEE 118 bus system, Fig. 11 shows how eliminating line 161, the most severe contingency, impacts the branch power flow. As seen, the loading of the adjacent transformers and lines increases as the above-mentioned line is removed. After a while, these outages isolate a section of the power system, which results in diverging power flow and blackouts.

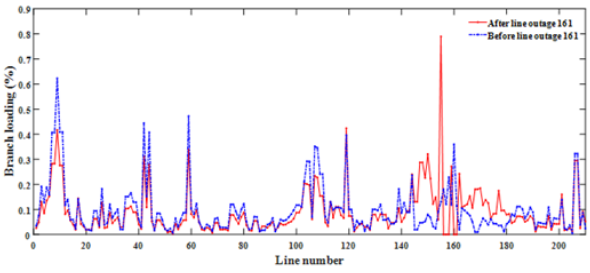

Fig. 11. Power flow variation after line outage 161.

5.3. Risk evaluation on modified IEEE 300 bus system

In this paper, the modified IEEE 300-bus system, which consists of 69 generators, 195 loads, and 416 branches, is used to illustrate the effectiveness of large-scale power systems. Also, the overall generation is 36418 MW and 15586 MVar, while the total load is 23526 MW and 7788 MVar under normal operating conditions. In the modified 300-bus network, a wind farm with a maximum generation capacity of 500 MW is added at buses 84, 143, 190, 236, 241, 7002, 7003, 7012, 7017, 7024, 7039, 7061, 7130, 7139, and 7166 [40]. Some of the contingencies with the highest risk level are reported in Table 4. Also, Fig. 12 shows the risk index for each line outage in the modified IEEE 300 bus system.

Table 4. Risk of the line outages for modified IEEE 300 bus system.

Line	From bus	To bus	Risk
L386	**223**	**224**	**0.725001**
L387	229	230	0.720115
L385	218	219	0.710916
L389	238	239	0.61881
L378	195	212	0.59849
L392	120	1200	0.573222
L391	119	1190	0.532857
L379	200	248	0.513247
L321	235	238	0.419986
L390	196	2040	0.419799
L380	201	69	0.389403
L388	234	236	0.377782
L408	7057	57	0.349282
L395	7061	61	0.336467
L409	7044	44	0.321108
L91	41	49	0.310675
L410	7055	55	0.307773
L100	45	74	0.298431
L374	164	155	0.284386
L177	118	119	0.273003
L404	7139	139	0.270387
L328	244	246	0.247636
L383	209	198	0.24616
L249	173	174	0.245234
L407	7039	39	0.241081
L174	115	122	0.24022
L405	7012	12	0.237211
L173	112	114	0.235707
L111	57	58	0.232738
L382	204	2040	0.226615

In order to maintain the power system's reliability and stability, it is necessary to keep the power generation equal to the demand at all times. For this goal, several smaller power networks are interconnected to form much bigger ones. The results also validate that the larger the network dimensions, the lower the probability of cascading failure and widespread blackouts. Moreover, Figs. 13 and 14 illustrate the out-of-service branch/node and the loss of load and generation. According to the obtained results, the modified IEEE 300 bus system has a high level of security for the specified line outages under N-1 criteria. Moreover, the risk value of line outage 386 is caused by the structural indices because all buses and lines are in service. This fact is presented in Fig. 15. Comparing the results of modified IEEE 118 and 300 buses reveals that the larger the network dimensions and the greater the number of connections, the lower the likelihood of cascading failures and blackouts.

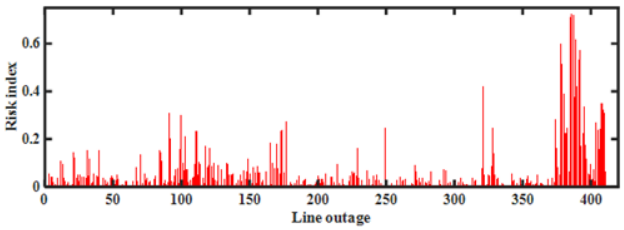

Fig. 12. Line outage risk for all branches of the modified IEEE 300 bus system.

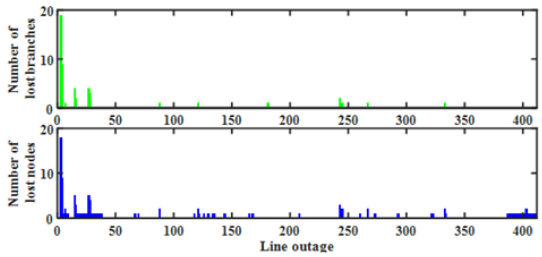

Fig. 13. Loss of branch and node for each line outage in modified IEEE 300 bus system.

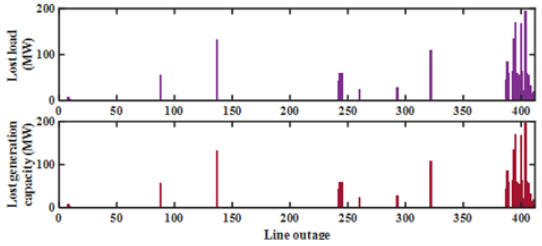

Fig. 14. Lost load and generation for each line outage in modified IEEE 300 bus system.

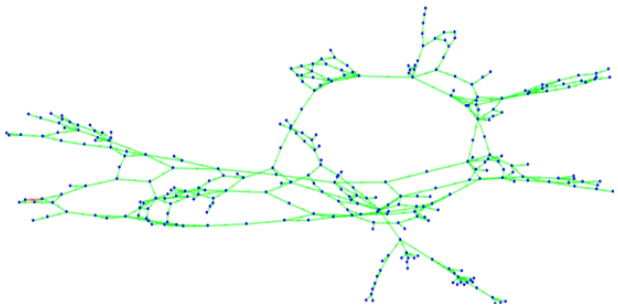

Fig. 15. Graph model of modified IEEE 300 bus system with line outage L386.

6. Conclusions

This paper provides a novel risk index for power system security assessment with a broad emphasis on integrating grid electrical and structural characteristics. For this goal, structural indices such as transmission efficiency and vulnerability have been combined with electrical features like cascading failure and its consequences. Also, the combined line outage and Weibull distribution functions have been used to model, respectively, the probability of line outages and wind speed uncertainty. The simulations were implemented on the modified IEEE 118 and 300 bus systems with wind farms to analyze the presented method's efficiency in the security assessment. This method can investigate the numerous contingencies to be studied in security assessment and rank the contingencies using the corresponding risk index. Furthermore, it enables transmission system operators to determine the most hazardous contingencies and provide preventive or corrective actions to address them. In summary, our approach is a step forward in traditional security assessment since it completes the N-1 credibility criterion with outages that lead to cascading failure. On the other hand, it determines the power system security status with less computational burden and improves the ability to deal with critical contingencies.

References

[1] E. Limouzadeh and A. Rabiee, "Security constrained reactive power scheduling considering n-1 contingency of transmission lines," *J. Oper. Autom. Power Eng.*, vol. 10, no. 1, pp. 66–70, 2022.

[2] M. Z. A. Bhuiyan, G. J. Anders, J. Philhower, and S. Du, "Review of static risk-based security assessment in power system," *IET Cyber-Phys. Syst.: Theor. Appl.*, vol. 4, no. 3, pp. 233–239, 2019.

[3] D. S. Kumar, H. Quan, K. Y. Wen, and D. Srinivasan, "Probabilistic risk and severity analysis of power systems with high penetration of photovoltaics," *Sol. Energy*, vol. 230, pp. 1156–1164, 2021.

[4] X. Li and Z. Qi, "Impact of cascading failure based on line vulnerability index on power grids," *Energy Syst.*, vol. 13, no. 4, pp. 893–918, 2022.

[5] C. Wang, P. Ju, F. Wu, S. Lei, and X. Pan, "Sequential steady-state security region-based transmission power system resilience enhancement," *Renewable Sustainable Energy Rev.*, vol. 151, p. 111533, 2021.

[6] Z. Ding, K. Yu, C. Wang, and W.-J. Lee, "Transmission line overload risk assessment considering dynamic line rating mechanism in a high-wind-penetrated power system: A data-driven approach," *IEEE Trans. Sustainable Energy*, vol. 13, no. 2, pp. 1112–1122, 2022.

[7] Y. Yin, T. Liu, L. Wu, C. He, and Y. Liu, "Day-ahead risk-constrained stochastic scheduling of multi-energy system," *J. Mod. Power Syst. Clean Energy*, vol. 9, no. 4, pp. 720–733, 2021.

[8] X. Li, Z. Yang, P. Guo, and J. Cheng, "An intelligent transient stability assessment framework with continual learning ability," *IEEE Trans. Ind. Inf.*, vol. 17, no. 12, pp. 8131–8141, 2021.

[9] Y. Wu, H. Chu, and C. Xu, "Risk assessment of wind-photovoltaic-hydrogen storage projects using an improved fuzzy synthetic evaluation approach based on cloud model: A case study in china," *J. Energy Storage*, vol. 38, p. 102580, 2021.

[10] X. Li, X. Zhang, L. Wu, P. Lu, and S. Zhang, "Transmission line overload risk assessment for power systems with wind and load-power generation correlation," *IEEE Trans. Smart Grid*, vol. 6, no. 3, pp. 1233–1242, 2015.

[11] M. Mehdizadeh, R. Ghazi, and M. Ghayeni, "Power system security assessment with high wind penetration using the farms models based on their correlation," *IET Renewable Power Gener.*, vol. 12, no. 8, pp. 893–900, 2018.

[12] N. Yorino, M. Abdillah, Y. Sasaki, and Y. Zoka, "Robust power system security assessment under uncertainties using bi-level optimization," *IEEE Trans. Power Syst.*, vol. 33, no. 1, pp. 352–362, 2017.

[13] S. Nangrani and S. Bhat, "Smart grid security assessment using intelligent technique based on novel chaotic performance index," *J. Intell. Fuzzy Syst.*, vol. 34, no. 3, pp. 1301–1310, 2018.

[14] S. K. Tiwary, J. Pal, and C. K. Chanda, "Ann-based faster indexing with training-error compensation for mw security assessment of power system," in *Energy Syst. Drives Autom.: Proc. ESDA 2019*, pp. 35–46, Springer, 2020.

[15] J. L. Cremer and G. Strbac, "A machine-learning based probabilistic perspective on dynamic security assessment," *Int. J. Electr. Power Energy Syst.*, vol. 128, p. 106571, 2021.

[16] T. Zang, S. Gao, T. Huang, X. Wei, and T. Wang, "Complex network-based transmission network vulnerability assessment using adjacent graphs," *IEEE Syst. J.*, vol. 14, no. 1, pp. 572–581, 2019.

[17] L. Guo, C. Liang, A. Zocca, S. H. Low, and A. Wierman, "Line failure localization of power networks part i: Non-cut outages," *IEEE Trans. Power Syst.*, vol. 36, no. 5, pp. 4140–4151, 2021.

[18] M. Alonso, J. Turanzas, H. Amaris, and A. T. Ledo, "Cyber-physical vulnerability assessment in smart grids based

on multilayer complex networks," *Sens.*, vol. 21, no. 17, p. 5826, 2021.

[19] S. Yang, W. Chen, X. Zhang, and W. Yang, "A graph-based method for vulnerability analysis of renewable energy integrated power systems to cascading failures," *Reliab. Eng. Syst. Saf.*, vol. 207, p. 107354, 2021.

[20] J. Beyza, E. Garcia-Paricio, and J. M. Yusta, "Ranking critical assets in interdependent energy transmission networks," *Electr. Power Syst. Res.*, vol. 172, pp. 242–252, 2019.

[21] P. Dedousis, G. Stergiopoulos, G. Arampatzis, and D. Gritzalis, "A security-aware framework for designing industrial engineering processes," *IEEE Access*, vol. 9, pp. 163065–163085, 2021.

[22] A. Almaleh and D. Tipper, "Risk-based criticality assessment for smart critical infrastructures," *Infrastruct.*, vol. 7, no. 1, p. 3, 2021.

[23] P. D. Hines, I. Dobson, and P. Rezaei, "Cascading power outages propagate locally in an influence graph that is not the actual grid topology," *IEEE Trans. Power Syst.*, vol. 32, no. 2, pp. 958–967, 2016.

[24] U. Nakarmi, M. Rahnamay Naeini, M. J. Hossain, and M. A. Hasnat, "Interaction graphs for cascading failure analysis in power grids: A survey," *Energ.*, vol. 13, no. 9, p. 2219, 2020.

[25] C. Chen, S. Ma, K. Sun, X. Yang, C. Zheng, and X. Tang, "Mitigation of cascading outages by breaking inter-regional linkages in the interaction graph," *IEEE Trans. Power Syst.*, vol. 38, no. 2, pp. 1501–1511, 2022.

[26] W.-L. Fan, X.-F. He, Y.-Q. Xiao, and Q.-Y. Li, "Vulnerability analysis of power system by modified h-index method on cascading failure state transition graph," *Electr. Power Syst. Res.*, vol. 209, p. 107986, 2022.

[27] K. Li, K. Liu, and M. Wang, "Robustness of the chinese power grid to cascading failures under attack and defense strategies," *Int. J. Crit. Infrastruct. Prot.*, vol. 33, p. 100432, 2021.

[28] B. Xie, X. Tian, L. Kong, and W. Chen, "The vulnerability of the power grid structure: A system analysis based on complex network theory," *Sens.*, vol. 21, no. 21, p. 7097, 2021.

[29] D. Zhang, L. Jia, J. Ning, Y. Ye, H. Sun, and R. Shi, "Power grid structure performance evaluation based on complex network cascade failure analysis," *Energ.*, vol. 16, no. 2, p. 990, 2023.

[30] D. Bose, C. K. Chanda, and A. Chakrabarti, "Vulnerability assessment of a power transmission network employing complex network theory in a resilience framework," *Microsyst. Technol.*, vol. 26, no. 8, pp. 2443–2451, 2020.

[31] H. F. Gharibeh, L. M. Khiavi, M. Farrokhifar, A. Alahyari, and D. Pozo, "Capacity value of variable-speed wind turbines," in *2019 IEEE Milan PowerTech*, pp. 1–5, IEEE, 2019.

[32] F. Hosseini, A. Safari, and M. Farrokhifar, "Cloud theory-based multi-objective feeder reconfiguration problem considering wind power uncertainty," *Renewable Energy*, vol. 161, pp. 1130–1139, 2020.

[33] F. Song, Y. Wang, L. Zhao, K. Qin, L. Liang, Z. Yin, and W. Tao, "Study on thermal load capacity of transmission line based on ieee standard," *J. Inf. Process. Syst.*, vol. 15, no. 3, pp. 464–477, 2019.

[34] I. Khan and M. Ghassemi, "A probabilistic approach for analysis of line outage risk caused by wildfires," *Int. J. Electr. Power Energy Syst.*, vol. 139, p. 108042, 2022.

[35] J. Sreedevi, G. Chethan, and P. L. Rao, "Voltage stability analysis of ieee118 bus system with wind penetration," *Power Res.-A J. CPRI*, pp. 17–21, 2022.

[36] "Assessment of reliability performance for the texas interconnection," tech. rep., Texas Reliability Entity, Inc, 2020.

[37] K. Pandiarajan and C. Babulal, "Fuzzy ranking based non-dominated sorting genetic algorithm-ii for network overload alleviation," *Arch. Electr. Eng.*, vol. 63, no. 3, 2014.

[38] H. Yuan, "A study on wide-area measurement-based approaches for power system voltage stability," *phD diss*, 2016.

[39] T. Nesti, J. Nair, and B. Zwart, "Temperature overloads in power grids under uncertainty: A large deviations approach," *IEEE Trans. Control Network Syst.*, vol. 6, no. 3, pp. 1161–1173, 2019.

[40] Y. Chen, S. M. Mazhari, C. Chung, S. O. Faried, and B. C. Pal, "Rotor angle stability prediction of power systems with high wind power penetration using a stability index vector," *IEEE Trans. Power Syst.*, vol. 35, no. 6, pp. 4632–4643, 2020.