Analysis of distribution network node vulnerability considering DGs

G B Li¹, W C Shi²³, X M Zhou¹, X M Li², Z Y Liu² and X D Wang²

¹Guangdong Power Grid Co., Ltd. Huizhou Huiyang Power Supply Bureau, Huizhou 516200, China
²School of Electrical Engineering, Wuhan University, Wuhan 430072, China
E-mail: 641336461@qq.com

Abstract. With the access of distributed generations (DGs), the safe operation of distribution network has attracted much more attention. How to find out the weak nodes in distribution network is urgent to be solved. In this paper, based on complex network theory and risk theory, the improved node degree, node betweenness and node voltage over-limit risk index are proposed. Analytic hierarchy process (AHP) method is used to give index weights of node degree, node betweenness and node voltage over-limit risk. And the comprehensive index of the vulnerability of distribution network nodes is obtained by weighting. Finally, the feasibility of the index is verified on the IEEE33 nodes system. And accessing DGs to simulation, the influence of DGs on the vulnerability of distribution network is qualitatively analyzed.

1. Introduction
With the continuous improvement of the economic level, the demand for electricity in all walks of life is also increasing. Once the power supply accident occurs in the power system, it will cause large power outages and huge economic losses. Since 2005, the global blackouts have occurred frequently. Nearly 100 million people were affected by the power grid failure in Indonesia. The United States also had a blackout in the same year, affecting 50 million people to use electricity normally. From these accidents, we can see that with the improvement of the power network complexity, it is more and more worthy of our attention and research to ensure the safe operation of power system. The concept of vulnerability was first proposed by American scholars as a description of the economic field. Nowadays, it is defined as finding out the weak points in the power network of the power system area [1]. When these weak points are subjected to external interference or influence, it is easy to cause cascading failures of components in the network, resulting in large-scale blackouts. Therefore, through vulnerability assessment and analysis, we can find out the weak points in the power network in advance, and improve these weak points, which will greatly reduce the possibility of power system blackouts.

The research on power grid vulnerability is mainly focused on the transmission network, and the research on the vulnerability of the distribution network is still in the initial stage [2]. This is mainly due to the fact that the distribution networks are mostly radial networks operating in open-loop mode. So the complexity is simpler than that of closed-loop transmission networks. However, with the development of new energy sources, the progress of wind power generation, photovoltaic power generation and energy storage technologies. The access to new energy sources makes the distribution network's safe operation of much concern.
The current vulnerability assessments are mainly based on the complex network theory. In literature[3], a weighted topology model is introduced on the basis of complex networks, and the vulnerability assessment is carried out on this model. Literature [4] analyzes the comprehensive vulnerability of the two aspects of the state and structure of the transmission network. Literature [5] combined with complex network theory and risk theory, put forward the comprehensive evaluation index of transmission network vulnerability. All the above studies aim at the transmission network without considering the impact of DGs.

Considering the characteristics of distribution network and the access of DGs, this paper puts forward a comprehensive evaluation index for the vulnerability of distribution network node based on complex network theory and risk theory. Firstly, the models of DGs are analyzed. Then, based on the complex network theory and risk theory, the comprehensive vulnerability index of distribution network nodes is proposed. Finally, combined with the IEEE33 nodes system and the access of DGs, the simulations are carried out.

2. DG models
In the power flow calculation of distribution network, excepting for the source node as a balanced node, the rest are regarded as PQ nodes. Since the node type of DG is determined by its model, a new node type will appear in the distribution network after the DG is connected. And the results of the power flow calculation will be changed accordingly. This paper only considers two DG models of wind power generation and photovoltaic power generation.

2.1. Wind power generation
The output characteristics of wind power generation are complex. Due to the randomness of wind speed, wind power generation has the characteristics of random fluctuation, uncontrollable, correlation and so on. Wind turbines mainly include asynchronous generators and synchronous generators, usually asynchronous generators are widely used. According to the probability density function of wind speed and the relationship between wind power and wind speed, we can see that the active power of wind power obeys the Weibull distribution of three parameters. Because wind turbines usually do not output reactive power, the shunt reactor is used to output reactive power and keep the power factor constant. Therefore, the wind power generation can be equivalent to the PQ node in the power flow calculation, which is equivalent to the negative load of the output [6], and its expression is as in equation (1).

\[
\begin{align*}
P &= -P_{DG} \\
Q &= -Q_{DG}
\end{align*}
\] (1)

2.2. Photovoltaic power generation
Photovoltaic power generation is mainly composed of photovoltaic cells and grid-connected inverters, in which the grid-connected inverter compensates reactive power in distribution network. The grid-connected inverter is divided into current control and voltage control type, and when the current control grid inverter is adopted, the dc side series of large inductance is equivalent to the constant current source, so it can be equivalent to PI node [7]. The output reactive power is as in equation (2).

\[
Q = \sqrt{I^2 (e^2 + f^2) - P^2}
\] (2)

Where \(I\) —the constant current that is injected into the grid, \(P\) — the constant active power of the output, \(e\) and \(f\) — the real and imaginary parts of the voltage of the photovoltaic system.

When the voltage controlled grid-connected inverter is used, its dc side and the combined capacitance are equivalent to the voltage source, so it can be equivalent to the PV node. Therefore, in the current calculation, the expression is as in equation (3).
\[
\begin{aligned}
P &= -P_{DG} \\
U &= U_{DG}
\end{aligned}
\]  

For PV nodes, special processing is required in the power flow calculation, but only in the calculation process is more complex than the PQ node, there is no substantial difference between them.

3. Node vulnerability indexes
The node comprehensive vulnerability indexes of distribution network proposed in this paper are based on complex network theory and risk theory. In this section, we introduce the vulnerability indexes of node based on complex network theory and risk theory respectively.

3.1. Vulnerability indexes of nodes based on complex network theory
By the definition of complex networks, the distribution network can be simplified as an undirected and weighted sparse graph with \( N \) nodes and \( L \) edges. Traditional complex network theory has its statistical characteristics, such as characteristic path length, degree, clustering coefficient and betweenness, which can be directly used as an index for vulnerability assessment of transmission network [8,9]. Considering that the structure of the distribution network is different from the transmission network, these statistical features need to be improved to meet the structure characteristics of the distribution network.

3.1.1. Improved node degree. The traditional node degree is defined as the number of nodes connected to the nodes. The average degree of the degree of all nodes can be obtained by means of the average value of the degree of all nodes. Node degree can reflect the importance of nodes in the network, that is, the bigger the degree of the node, the more important and more vulnerable in the network [10]. When taking the access of DGs into account, since nodes connecting DGs are simplified as PQ nodes or PV nodes during power flow calculation, the number of system nodes is not changed. Therefore, the node degree of DGs access nodes should be increased by 1 to calculate. The formula is as in equation (4).

\[ D_i = D_{DG} + 1 \]  

where \( D_i \)—the degree of access to the DG node, \( D_{DG} \)—Node original node degree.

Because the distribution networks are mostly radial network, they are sparser than the transmission networks. Considering the degree of its node, it is difficult to compare the difference between the nodes with the same degree. In this paper, the idea of cohesion is introduced, and the influence on nodes connected to node \( i \) is taken into account. The degree of nodes is proposed as in equation (5).

\[ Nk_i = \frac{D_i}{\bar{D}} \sum_{j \in V_{ad}} D_j \]  

where \( \bar{D} \)—the average degree of network nodes, \( V_{ad} \)—the set of all nodes connected with node \( i \).

3.1.2. Improved node betweenness. The traditional node betweenness is defined as the number of shortest paths through that nodes. The betweenness is used in the social network as early as possible. It is used to measure the importance of nodes in the network. The larger the betweenness of node is, the more important the node is to assume more intermediary functions in the network [11]. The traditional betweenness of node assumes that the power flow of the system is calculated according to the shortest path, ignoring the objective flow in the distribution networks. In order to reflect the factors such as the objective power flow distribution and node capacity in the distribution network, and reflect the actual situation of the power transmission between generators and loads to the occupancy of each node, we define the betweenness of node [12,13] as in equation (6).
\[ Nb_i = \frac{1}{S_b} \sum_{m \in \mathcal{M}, n \in \mathcal{N}} \sqrt{S_m S_n} \alpha_{mn}(i) \]  

(6)

where \( \alpha_{mn}(i) = \begin{cases} \frac{1}{2} \sum_{j \in \mathcal{V}_{mn}} |I_{mn}(i, j)| & (i \neq m, n) \\ 1 & (i = m, n) \end{cases} \)

where \( S_b \) — the system reference capacity, \( m \) — the generator node, \( n \) — the load node, \( S_m \) — the actual power of generator node, \( S_n \) — the actual power consumption of load node, \( I_{mn}(i, j) \) — the current produced on the path of \( i-j \) after the unit power supply is injected into the \( m-n \) node, \( \mathcal{V}_{ad} \) — the set of all nodes connected with node \( i \).

Taking the influence of DGs into account, the DG simplified as the PQ node is calculated as the load and the DG simplified as the PV node is calculated as the generator when solving the node betweenness. Therefore, the PQ type DG has no effect on the number of nodes. The PV node is regarded as a generator node, so it will increase the betweenness of nodes and reflect the objective trend.

3.2. Node voltage over-limit risk index based on the risk theory

The indexes proposed based on complex network theory mainly reflect the weak nodes in the distribution network structurally, and do not take into account the possible risks of failure or power quality failure in the system. The risk theory takes into account the possibility of the failure of the system and the severity of the fault. This paper introduces risk theory to make up for the deficiencies of complex network theory [14-16].

The node voltage over-limit risk of the node reflects the possibility and severity that the bus voltage in the distribution network is too high or too low. The access of DGs will cause reactive power of the system to change, resulting in the distribution network voltage changes. When the DG is connected to the users’ side or to the load side, it is possible to reverse the power flow to counteract the original voltage drop and increase the voltage. When DGs are connected to the downstream of the regulator, the loads of the pressure drop compensation device are less than before, so that the target voltage values of the voltage compensation are lower than the actual setting values of the specified standard of the feeder terminal voltage, resulting the voltages are lower than that of DGs [17].

Considering the voltage offset in the normal operation of the 10kV line at \( \pm 7\% \), the node voltage over-limit risk index is as in equation (7).

\[
Nu_i = \begin{cases} 
    e^{(u_i - 1.07)} & u_i > 1.07 \\
    1 & 0.93 \leq u_i \leq 1.07 \\
    e^{(0.93 - u_i)} & u_i < 0.93 
\end{cases}
\]

(7)

where \( u_i \) — the per-unit value of voltage.

When the node voltage is \( 0.93 \text{pu} \leq u_i \leq 1.07 \text{pu} \), the risk of failure is 1. When the voltage is \( u_i > 1.07 \text{pu} \), as the voltage continues to increase, the voltage over-limit risk increases exponentially, and the greater the possibility of failure. When the voltage is \( u_i < 0.93 \text{pu} \), as the voltage continues to decrease, the voltage over-limit risk increases exponentially, and the greater the possibility of failure.

4. Node comprehensive vulnerability index

It is hard to make a scientific and comprehensive judgement of node vulnerability based on single node vulnerability index. It is very important to choose the appropriate node vulnerability indexes to solve the vulnerability of nodes. Based on the complex network theory, the node vulnerability indexes...
mainly analyze the vulnerability of the nodes structurally. Based on the risk theory, the node voltage over-limit risk index analyzes the vulnerability of the nodes from the risk of failure. Combined with the two, the comprehensive vulnerability index of the node can make up for the deficiency of the two parts and make comprehensive judgement.

In this paper, we use the analytic hierarchy process (AHP) to give weight to the indexes. Analytic hierarchy process decomposes decision problems into different hierarchies according to the general objectives, the different levels of objectives, the evaluation criteria, and the specific options. Then, by using the method of finding the eigenvectors of the judgement matrix, the priority weights of each element of each level to the elements of the upper level are obtained. Finally, the weighted sum method is used to merge the final weights of the alternatives to the total target.

By consulting experts, it is equally important to set the node degree and node betweenness. And the node voltage over-limit risk is more important than them. Using the analytic hierarchy process, we can get the comparison matrix:

\[
\begin{bmatrix}
1 & 1 & \frac{1}{3} \\
1 & 1 & \frac{1}{3} \\
3 & 3 & 1 \\
\end{bmatrix}
\]

The matrix satisfies the consistency requirements, and the weights of the node degree, the betweenness and the node voltage over-limit risk are obtained as 0.2, 0.2, and 0.6. The comprehensive vulnerability index of distribution network of node \(i\) obtained by AHP is as in equation (8).

\[
N_i = 0.2 \times N_{k_i} + 0.2 \times N_{b_i} + 0.6 \times N_{u_i}
\] (8)

Because of the differences in the units and orders of magnitude of the above indexes, they can not be added directly. The units and orders of the indexes should be unified first. In this paper, the maximum value of each indexes is used as a benchmark for normalization, and the data is normalized to the interval in \([0,1]\).

5. Simulation analysis
This paper uses the standard IEEE33 nodes system for simulation. The distribution network is a 10kV network, with a total of 33 nodes, 32 branches and 5 contact switch branches. The source node (node 1) is set as the balance node, the reference voltage is 12.66kV, and the system power base is 10MVA. The topology of the IEEE33 nodes distribution network is shown in figure 1.

![Figure 1: IEEE33 node distribution network topology.](image)

5.1. IEEE33 nodes distribution system
In figure 1 the contact switch branches are disconnected, and the simulation calculation is carried out in the open loop operation. The results of each indexes calculation are shown in figure 2. And the results of node comprehensive vulnerability index is shown in table 1 by ranking.
Figure 2. The result of the each indexes.

Table 1. The results of node comprehensive vulnerability index.

| Node | $N_i$ | Node | $N_i$ |
|------|-------|------|-------|
| 2    | 0.9635| 10   | 0.7081|
| 1    | 0.9158| 11   | 0.7078|
| 3    | 0.8835| 12   | 0.7060|
| 6    | 0.8244| 29   | 0.7045|
| 19   | 0.7818| 30   | 0.7018|
| 23   | 0.7700| 13   | 0.7009|
| 4    | 0.7644| 22   | 0.6994|
| 5    | 0.7579| 14   | 0.6993|
| 20   | 0.7577| 31   | 0.6987|
| 26   | 0.7464| 15   | 0.6982|
| 7    | 0.7399| 16   | 0.6971|
| 21   | 0.7380| 25   | 0.6814|
| 24   | 0.7222| 32   | 0.6789|
| 27   | 0.7199| 17   | 0.6765|
| 8    | 0.7167| 33   | 0.6406|
| 9    | 0.7118| 18   | 0.6379|
| 28   | 0.7107|

In figure 2, different colors mean different nodes. The height of the histogram means the calculated values of each index.

From figure 2 and table 1, we can see that the vulnerability of node 1 and node 2 are large, because the degree, betweenness are relatively high, and the node voltages are about 12.66kV. After weighting, the comprehensive vulnerability are relatively high. The vulnerability of the remaining nodes decrease with the topology structure to the tail nodes, and it can be seen that the vulnerability of the tail nodes are the lowest.

In order to verify the feasibility of the proposed index, the method of [18] is used to calculate the IEEE33 nodes system. Compared with the calculation results of this paper, the first 10 nodes are compared and ranked in table 2. As can be seen from table 2, the order of the literature [18] method is roughly the same as the method of this article, but there are some differences. Because the indexes mentioned in the literature only consider the factors of the network structure unilaterally, without considering the influence of power, voltage and so on. In the case of complex networks with large
nodes, the result of that method is not accurate enough, and the method in this paper is more comprehensive, considering the influence of power flow and fault risk. Through the above comparison, the feasibility of this method is verified.

Table 2. Node vulnerability ranking.

| Node Ranking | This paper | literature [18] |
|--------------|------------|-----------------|
| 2            | 1          | 2               |
| 1            | 2          | 2               |
| 3            | 3          | 3               |
| 6            | 6          | 6               |
| 19           | 4          |                 |
| 23           | 5          |                 |
| 4            | 19         |                 |
| 5            | 23         |                 |
| 20           | 26         |                 |
| 26           | 7          |                 |

5.2. IEEE33 nodes power distribution system with DGs

In order to analyze the influence of DGs on the distribution network vulnerability, two types of DGs, PQ and PV, are connected to the IEEE33 nodes system. Nodes 22 and 25 are all connected to the PQ nodes with complex power $S=0.63+j0.405\text{MVA}$, and node 9 is connected to PV nodes with active power $P=0.05\text{MW}$ and voltage 1.0pu. Node 16 is connected to PV node with active power $P=0.07\text{MW}$ and 1.02pu voltage. After accessing the DGs, the topology diagram of the distribution network is shown in figure 3, and the results of the indexes calculation are shown in figure 4 and table 3.

Figure 3. Network topology after access to DGs.

Figure 4. The results of the each indexes after accessing to DGs.
Table 3. The result of node comprehensive vulnerability index after accessing to DGs.

| Node | $N_i$ | Node | $N_i$ |
|------|-------|------|-------|
| 1    | 0.8228| 7    | 0.6146|
| 2    | 0.8186| 15   | 0.6146|
| 3    | 0.7844| 25   | 0.6106|
| 19   | 0.7039| 11   | 0.5962|
| 6    | 0.6964| 12   | 0.5955|
| 21   | 0.6731| 27   | 0.5954|
| 23   | 0.6719| 17   | 0.5953|
| 20   | 0.6717| 14   | 0.5951|
| 4    | 0.6579| 13   | 0.5951|
| 24   | 0.6473| 29   | 0.5951|
| 5    | 0.6446| 30   | 0.5951|
| 22   | 0.6382| 31   | 0.5951|
| 9    | 0.6342| 28   | 0.5951|
| 16   | 0.6338| 32   | 0.5760|
| 26   | 0.6200| 18   | 0.5379|
| 10   | 0.6153| 33   | 0.5379|
| 8    | 0.6148|      |       |

After accessing to DGs, the ranking of vulnerability of the nodes has changed. The changes of the degree and the betweenness of each node are small. Since the PV node clamps the node voltage within a safe range, the node voltage over-limit risk index across the entire distribution system becomes smaller. In order to analyze the impact of DGs on the original system, the vulnerability ranking of nodes is compared as shown in figure 5. The higher ranking means the more fragile the nodes.

![Comparison of vulnerability of DG nodes.](image)

Figure 5. Comparison of vulnerability of DG nodes.

It can be seen from figure 5 that the ranking of node 1-3 are basically the same. The PV type distributed power supply has been connected to the node 9, and its vulnerability is greatly increased. From each indexes, it can be seen that the change is mainly caused by the the increase of node degree and the node betweenness. The node 11-14 are located between the PV nodes, and their vulnerability are significantly reduced, which are due to the lower risk of the node voltage. Accessing to the PV-type distributed power supply at node 16 has the same significant increase in vulnerability as node 9. Node 17,18 slightly increase their vulnerability due to a slight increase in the number of nodes. The vulnerability of node 19-22 increase because the betweenness of node 19-22 increase. The node 25 accesses the PQ node, resulting in increased vulnerability. The loads of nodes 23 and 24 are large,
which can reduce the risk of node voltage over-limit of PQ nodes, reducing the comprehensive vulnerability of nodes.

5.3. The influence of DGs on distribution network vulnerability
In the 5.2 quarter, the 19-22 branches and 23-25 branches access the same DG of PQ type, but the results of two branches are different: the overall node vulnerability of 19-22 branches is improved, while the overall node vulnerability of 23-25 branches decreases. To clarify the influencing factors, we only connect the 22 and 25 nodes to the DG of PQ type (excluding the influence of PV nodes), and compare it with the vulnerability of the original distribution network, which is shown in figure 6.

![Figure 6. Comparison of node vulnerability access to DG of PQ type.](image)

From figure 6, we can see that the comprehensive vulnerability of node 19-22 are significantly improved, and the comprehensive vulnerability of node 23-25 are obviously reduced, which are the same as that of 5.2 quarter. For more detailed analysis, the specific indexes of node 19-25 are shown in table 4.

Table 4. Calculation results of node vulnerability indexes of node 19-25.

| Node | $N_{k_i}$ | $N_{b_i}$ | $N_{u_i}$ | $N_{i}$ |
|------|-----------|-----------|-----------|--------|
| 19   | 0.4762    | 0.0114    | 0.9612    | 0.6742 |
| 20   | 0.3810    | 0.0005    | 0.9988    | 0.6756 |
| 21   | 0.3810    | 0.0004    | 0.9997    | 0.6761 |
| 22   | 0.1905    | 0.0003    | 1.0018    | 0.6393 |
| 23   | 0.4762    | 0.0220    | 0.9831    | 0.6895 |
| 24   | 0.3810    | 0.0007    | 0.9817    | 0.6653 |
| 25   | 0.1905    | 0.0005    | 0.9842    | 0.6287 |

Table 4 shows that: Due to the uneven distribution of active power, the node voltage over-limit risk of node 19-22 are significantly higher than node 23-25. That is, the output of node 22 to DG is much larger than the absorption of the branch, so the transmission power of nodes increases. In order to verify the above conclusion, the power of PQ node is set to S=0.36+j0.16MVA according to the actual cancellation capacity of node 19-22, and the calculation is carried out to compare with the original network, see figure 7.

It can be seen from figure 7 that the overall vulnerability of nodes 19-22 have changed. The overall vulnerability of nodes 19 and 20 have decreased, and the overall vulnerability of nodes 21 and 22 have been significantly lower than that of figure 4. This shows that the capacity of DG will affect the
overall node vulnerability, the specific effect should be analyzed according to the specific load.

In the power flow calculation, the reactive power is determined by the voltage, so the reactive power of the PQ nodes can be selected according to the network voltage and the load conditions, and finally it can have the same stable voltage as the PV nodes.

Through the above analysis, the impact of DGs on the vulnerability of distribution network is mainly affected by the location and capacity. Therefore, the above two factors should be considered when accessing distributed power. The deficiency of this paper is that the timing characteristics of DG can not be considered, so it can not reflect the impact of the actual operation of distribution system on the node vulnerability of distribution network.

6. Conclusion
Based on complex network theory and risk theory, a comprehensive vulnerability index of distribution network considering DGs is proposed. The vulnerability of distribution network is considered from two aspects of structure and operation risk. Using AHP to weight the proposed indexes, we can get the comprehensive vulnerability index of nodes. Through the simulation of IEEE33 nodes system and compared with the literature [18], the feasibility of the index is verified. In this paper, the IEEE33 nodes system is randomly connected to DGs, and the simulation are carried out. The qualitative analysis of the influence of DG is also made. The obtained results are basically consistent with reality, which verifies the practicality and scientificity of the evaluation indexes proposed in this paper.

References
[1] Shi Y, Zhang D and Diao Z 2018 An improved parallel maximum flow approach for vulnerability analysis of power system Int. Conf. Big Data Analysis (ICBDA), Shanghai China, pp 397-401
[2] Wei X, Gao S, Huang T, Bompard E, Pi R and Wang T 2018 Complex network-based cascading faults graph for the analysis of transmission network vulnerability IEEE T. Ind. Inform. 5 1
[3] Guo Y, Cao J, Duan R, Duan R and Li S 2012 Power grid vulnerability identifying based on complex network theory 2nd Int. Conf. Instrum. Meas. Comput. Commun. Contr. IEEE Computer Society, Guangzhou China, pp 474-7
[4] Wei Z, Liu J, Zhu G, Zhu K, Liu L and Fang T 2009A new integrative vulnerability evaluation model to power grid based on running state and structure Autom. Electr. Power Syst. 33 11-4
[5] Xiao S, Zhang J and Xiao H 2013 Vulnerability assessment of a regional power grid based on complex network theory and risk theory Power Syst. Clean Energy 29 21-8
[6] Vinothkumar K, Selvan M P and Srinath S 2010 Impact of DG model and load model on placement of multiple DGs in distribution system Int. Conf. Ind. Inform. Syst. Chengdu, pp 508-13
[7] Liu C, Xu Q, Chen Z, Bak C and Claus L 2012 Vulnerability evaluation of power system
integrated with large-scale distributed generation based on complex network theory

Universities Power Engineering Conference, Brisbane, Queensland, Australia, pp1-5

[8] Dong X, Nyberg T R, Hämäläinen P, Xiong G, Liu Y and Hou J 2015 Vulnerability analysis of smart grid based on complex network theory Int. Conf. Inform. Sci. Tech. Zürich, Switzerland, pp 525-9

[9] Beyza J, Yusta J M, Correa G J and Ruiz H F 2018 Vulnerability assessment of a large electrical grid by new graph theory Latin America Transactions 16 2

[10] Chowdhury T, Chakrabarti A and Chanda C K 2016 Analysis of Vulnerability indices of power grid integrated DG units based on Complex Network theory Annual IEEE India Conference,Inida, pp 1-5

[11] Zhao H, Hu Y, Ai X Yand Yu H 2017 Fault detection of associated complex systems using integrated complex network theory with SVM Int. Conf. Comput. Commun. Chengdu, China, pp 2659-64

[12] Koushik S, Pang C and Yang L 2017 Optimal location for single and multiple DG based on vulnerability index in smart distribution system Power & Energy Society General Meeting,Chicago,USA, pp 1-5

[13] Han S and Li P 2017 Vulnerability assessment of navigation station equipment network based on complex network theory Conference of the IEEE Ind. Electr. Soc. Beijing, China, pp 6940-5

[14] Jia Y, Liu R, Han X S and Wang P 2017 Risk assessment of cascading failures in power grid based on complex network theory International Conference on Control, Automation, Robotics and Vision, Phuket, Thailand, pp1-6

[15] He W, Hua G, Zheng H, Fang W and Liu H 2017 Quantitative method to pre-assess vulnerability for microgrid based on probability theory J. Eng. 2017 1113-7

[16] Qi H, Shi L, Ni Y, Yao L and Bazargan M 2014 Study on power system vulnerability assessment based on cascading failure model Pes General Meeting/Conference & Exposition, MD, USA, pp 1-7

[17] Surisunthon S and Tayjasanant T 2011 Impacts of distributed generation's locations, sizes, operation modes and transformer connections on voltage sag assessment TENCON 2011 - 2011 IEEE Region 10 Conference, Indonesia, pp 893-7

[18] Wu H, Peng M, Zhang H, Zhu L, Che W and Liu Z 2017 Vulnerability assessment for distribution network based on complex network theory Complex System and Complexity Science 14 38-45