Geodesic Vulnerability Approach for Identification of Critical Buses in Power Systems

Jesus Beyza, Eduardo Garcia-Paricio, Hector F. Ruiz, and Jose M. Yusta

***Abstract*—One of the most critical issues in the evaluation of power systems is the identification of critical buses. For this purpose, this paper proposes a new methodology that evaluates the substitution of the power flow technique by the geodesic vulnerability index to identify critical nodes in power systems. Both methods are applied comparatively to demonstrate the scope of the proposed approach. The applicability of the methodology is illustrated using the IEEE 118-bus test system as a case study. To identify the critical components, a node is initially disconnected, and the performance of the resulting topology is evaluated in the face of simulations for multiple cascading faults. Cascading events are simulated by randomly removing assets on a system that continually changes its structure with the elimination of each component. Thus, the classification of the critical nodes is determined by evaluating the resulting performance of 118 different topologies and calculating the damaged area for each of the disintegration curves of cascading failures. In summary, the feasibility and suitability of complex network theory are justified to identify critical nodes in power systems.**

***Index Terms*—Power system, critical node, complex network theory, cascading failure, load flow.**

I. Introduction

IN recent years, power systems have become one of the most important critical infrastructures for the development of any country. These systems may be prone to undesirable events such as equipment failures, human errors, procedure failures, or natural disasters that have the potential to affect the combined operation of assets and lead to serious consequences for the whole system [1]. For example, an event in a substation could degrade the performance of power systems and trigger a series of cascading events caused by the malfunction of critical facilities [2]. The blackouts in the United States and Canada in 2003, Brazil and Paraguay in 2009 and India in 2012 illustrate the severe effects of these unwanted events [3]-[5].

Researchers have increasingly focused on the mechanisms that explain the previous incidents, as they have found that the disruption of certain buses could severely affect the normal performance of the infrastructure [3]. Therefore, it is necessary to identify critical components that could have catastrophic consequences on the power grid if eliminated. The identification of these assets alone could increase the reliability of power systems and reduce the risk of blackouts [6].

To this end, various methods have been used in literature, among which multi-criteria analysis techniques [7], mixed-integer linear programming [8]-[10], Monte Carlo techniques [11], controllability theory [12] and fault chain theory [13] have been highlighted. More recently, a new methodology has been employed for the identification of critical assets in power networks, known as complex networks or graph theory [14]-[19]. This technique models the electrical networks as a graph composed of nodes and links. The nodes represent electrical substations, and the links represent transmission lines [20]. The basic concept behind this method is to use statistical indicators or centrality measures that describe the topological characteristics of the systems. Until now, the latest developments in graph theory have provided new guidelines for the study of power systems [21]. The following is a summary of the most notable works in this research area.

Reference [14] provides a graphic representation of a power system composed of vertices and edges in which the latter have been weighted by the admittances of transmission lines of the infrastructure. In addition, the use of alternating current (AC) power flow model is combined to propose a nodal degree index, which is useful for determining critical buses. Similarly, [16] proposes the weighted entropy index to identify the most vulnerable transmission lines of the electrical network. In some cases, the addition of some assets could cause a decrease in power system performance, and small changes in network topology could drastically increase the vulnerability [22], [23]. Thus, stakeholders should consider making new investments to increase the robustness of the infrastructure against cascading failures or unwanted events. Several works have followed the same research line using

Manuscript received: November 15, 2018; accepted: September 25, 2019. Date of CrossCheck: September 25, 2019. Date of online publication: March 12, 2020.

This work was supported by TECNM-Mexico (No. 6520.18-P) and the Ministry of Economy and Competitiveness, Spain (No. ENE2016-77172-R).

J. Beyza and H. F. Ruiz are with PGIIE, Instituto Tecnologico de Morelia, Avenida Tecnologico 1500, Lomas de Santiaguito, 58120, Mexico, and J. Beyza is also with the Department of Electrical Engineering, University of Zaragoza, C/Maria de Luna 3, 50018, Spain (e-mail: jbbcia4@hotmail.com; hfruiz53@yahoo.com.mx).

E. Garcia-Paricio and J. M. Yusta (corresponding author) are with the Department of Electrical Engineering, University of Zaragoza, C/Maria de Luna 3, 50018, Spain (e-mail: egarciap@unizar.es; jmyusta@unizar.es).

DOI: 10.35833/MPCE.2018.000779

different case studies [18], [19].

Some research works only apply system connectivity and purely topological indices [15]. Others propose the use of combined indicators such as the hybrid flow betweenness approach, which considers the power flows and the reactance of transmission lines [17], [21]. The electrical and connectivity parameters of the networks are also evaluated considering the properties of the components and the mutual effects between facilities [2], [24].

Similarly, other academics model the power systems as a weighted directed graph, through which they construct incidence matrices of buses and lines to determine the most critical buses [25]. Other recent works consider the inherent structural characteristics of the power systems by using multi-dimension graphs, sensitivity approaches, eigenvalues as well as new centrality indices formulated from the k-shell decomposition method and response matrices of both the load and generator nodes [26]-[30]. We find that the graphical representation of the electrical network facilitates a prompt identification of weak elements whose disruption could have an undesirable impact on power system stability.

Given the extensive development of the communication, computing, and control technologies, power systems become smart grids, requiring the reinforcement of protection and reliability strategies, and a detailed analysis of new contingencies in the face of various types of threats [31]. Therefore, it is necessary to discuss and analyze the vulnerability of smart grids, considering the new assets and cyber layers that compose them. In this sense, the complex network theory has many applications, mainly aiming at quantifying the infrastructure robustness against physical sabotage, cyberattacks, and simultaneous attacks [32]-[34].

From a broader view of the literature, the results obtained in this research area and determined by graph theory show that high-voltage electrical substations are critical from the topological perspective for power flow transmission [35], [36]. Also, critical regions in power systems have been identified. In most cases, the physical topology and interaction between facilities significantly affect the spread of failures [37], [38]. Likewise, it shows that certain sets of highly connected buses could contain critical information about the cascading process, so that their protection would prevent the propagation of these undesirable events [39]. Some works recently incorporate the concept of resilience into the study of power systems [40].

On the contrary, other works apply the bi-level attacker-defender interdiction model to address electrical network vulnerability and identify critical assets [41]. These multi-level models aim to estimate the worst-case scenario of the power grid for any feasible protection strategy. In the meantime, modal decomposition approaches for determining the dynamic model of the electrical network and finding generators, loads, and weak zones have also been utilized [42]-[44].

Finally, some remaining works employ the concept of sparse optimization to formulate a decentralized solution algorithm that identifies the most critical buses that contribute to the dynamics of the system [45], [46]. Other works calculate the fast voltage stability index (FVSI) to determine critical buses and critical lines [47], [48]. The latter approach uses several electrical parameters of the network.

In summary, the following shortcomings can be found in the literature related to critical bus identification in power systems:

1) Although some techniques used in the identification of critical components are well established in [7]-[13], they require high computational complexity.

2) The works use the electrical parameters of the systems [2], [17], [21], [24].

3) The works using graph theory do not validate their results against load flow studies [14]-[17].

4) Power systems are now becoming smart grids, thus more studies should be done focusing on this new area, especially on cybersecurity, reliability, and physical sabotage [31].

In this paper, we aim to identify the critical buses of power grids according to the behavior of networks in terms of cascading failures. The main purpose of identifying these assets is to improve their protection and, consequently, to reduce power grid vulnerability. The consequences are investigated when the system is prone to random disruptions such as equipment failures, human errors, or procedure failures, which could lead to a process of network decomposition and cause a total collapse in the performance of power systems [49]. Two types of vulnerability are found in literature: functional and structural. The first one incorporates the technical parameters of the infrastructure, and the second one involves the negative performance of the network topology [50]. Thus, unlike works which deal in-depth with some of the most critical blackouts and can be classified as part of functional vulnerability studies [51]-[54], this paper is developed from a structural vulnerability, as it only considers the study of the topological structure of the system.

We define structural vulnerability as the lack of robustness and resilience of the power grid against high-impact events. Robustness indicates that the power system can continue to operate when it is under attack or disturbance, and resilience indicates that the power system can be adapted for a new steady condition after contingency. Structural vulnerability is related to the decrease in the performance and efficiency of the electrical network after some of its assets have been disrupted.

The drop of infrastructure performance is measured using the geodesic vulnerability index $\bar{v}$. Because it enables the performance measurement of an electrical network subject to contingency events and allows effective comparisons in the evolution of the successive iterations of bus disconnections in a power system in relation to its stable condition before the on-set of contingencies [55]. Another relevant contribution of this work is the need to evaluate the effectiveness and validity of the results achieved with the graph index. Therefore, parallel to the calculation of the topological indicator, direct current (DC) load flows are executed on the electrical networks resulting from the bus disconnections. We consider this technique because we are only interested in the calculation of active power flow in the transmission lines after eliminating a substation, although other techniques such as continuous power flows could be used [56]. Thus, the load shedding index LS is used to quantify the total real power supplied within the electrical infrastructure [57], and the results are compared to determine the accuracy achieved by the statistical indicator, which justifies the use of graph theory as a faster and more efficient analysis method than the power flow technique for identifying critical nodes in electrical networks. Finally, a dimensionless measure is proposed to quantify the effect of each disintegration curve as a consequence of the initial elimination of an bus and to classify critical nodes in power systems.

Considering these aims, the main contributions of this paper can be summarized as follows:

1) A detailed procedure based on graph theory is presented to identify critical buses in power systems. The methodology is effective and flexible.

2) The suitability of $\bar{v}$ index is demonstrated as a good substitute for load flow studies to assess the vulnerability of power grid topologies against cascading effects.

3) A measure called damage area is proposed to classify the critical buses.

4) In this work, 118 networks of the same test system are analyzed.

This paper is organized as follows: Section II presents a cascading failure model to identify the critical buses of the electrical networks. The indices used are mentioned, and the proposed methodology is detailed. Section III describes a case study and reports the results achieved with the proposed methodology. Finally, the conclusion is presented in Section IV.

II. Cascading Failure Modeling to Identify Critical Nodes

This section describes the proposed methodology to identify the critical assets of electrical infrastructures.

A. LS Index

From the perspective of the complex network theory, the cascading failure modeling consists of eliminating nodes and links in a graph that continually changes its topology. Under this assumption, a power system is considered in this paper as a graph subject to random nature events. Therefore, when electrical networks are exposed to this type of event, it may be possible to lose critical assets that play vital functions in system operation.

To quantify the devastating effect of the aforementioned random failures, *LS* is proposed. This measure is presented in [57]. Note that one of the objectives of this paper is to validate the accuracy of the results obtained by graph theory versus power flow indicators. Thus, *LS* is used as a comparison metric relative to the graph index, which is calculated as:

$$LS = \frac{\sum_{i} \sqrt{\left(P_{Di}^{LC}\right)^2}}{\sum_{i} \sqrt{\left(P_{D}^{BC}\right)^2}} \tag{1}$$

where P_{Di}^{LC} is the real power supplied within the electrical network after an electrical substation i is eliminated; and P_{D}^{BC} is the total real power supplied within the electrical network for the base case.

LS varies between 0 and 1. As *LS* tends to be 0, the impact on the energy supplied to the electrical infrastructure increases.

B. $\bar{v}$ Index

A graph adjacency matrix can describe a power system as follows: $\boldsymbol{A}_{mn} = [N \times N]$, where m and n represent the links between different pairs of nodes and N equals the total number of vertices [58]. Note that the nodes indicate electrical substations and the links indicate power transmission lines.

When the electrical infrastructure is represented as a graph, one can calculate statistical indices that describe the physical or topological characteristics of the network [59]. For example, the nodal degree index k provides a measure for the connectivity of the nodes, the average nodal degree $\bar{k}$ represents a relative indicator for showing how meshed the system is, the shortest average path $\bar{l}$ measures the accessibility of one node in relation to another, and the network diameter d is the longest path in the network. Similarly, the geodesic efficiency index $\bar{e}$ allows to quantify the efficiency with which the information can be exchanged within a network [55]. The latter indicator determines the $\bar{v}$ index used in this work.

The $\bar{v}$ index measures the performance of the network against contingencies because it normalizes $\bar{e}$ and balances the process of disintegration of the network. $\bar{v}$ is calculated as:

$$\bar{v} = \frac{\sum_{i \neq j} \frac{1}{d_{ij}^{LC}}}{\sum_{i \neq j} \frac{1}{d_{ij}^{BC}}} \tag{2}$$

where d_{ij}^{LC} is the geodesic distance between pairs of nodes in the graph after each iteration of node elimination; and d_{ij}^{BC} is the geodesic distance between pairs of nodes in the graph for the base case.

The geodesic distance describes the shortest direct distance between two nodes by counting the minimum number of vertices that must be crossed to join them [60].

Similar to *LS*, $\bar{v}$ varies between 0 and 1. The smaller the value of this measure, the greater the impact on the decomposition of the graph.

C. Algorithm Used to Identify Critical Buses

In this paper, the critical components of an electrical network are identified through a cascading failure disintegration process. In this case, the complex network theory is applied in addition to the classical power flow technique. A graphical representation of a power system composed of nodes and edges is shown in Fig. 1. It is assumed that the power grid has n_g electric generators that provide enough energy to keep the system load in operation.

Figure 2 shows the proposed algorithm to identify critical buses by disintegrating the power system through the evolution of *LS* and $\bar{v}$ presented in (1) and (2), respectively.

Cascading events are simulated by eliminating nodes randomly. In this process, multiple iterations of $N-k$ contingencies are carried out on an electrical network that continually changes its topology with the elimination of each node. Since it is not possible to run the power flows without the slack generator, one cannot delete this node during the execution of the algorithm.

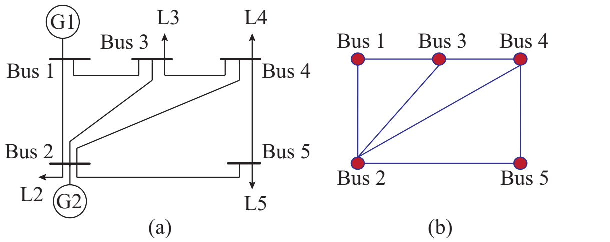

Fig. 1. Graphic representation of an electrical network composed of nodes and links. (a) Sample power system. (b) Power system as a graph.

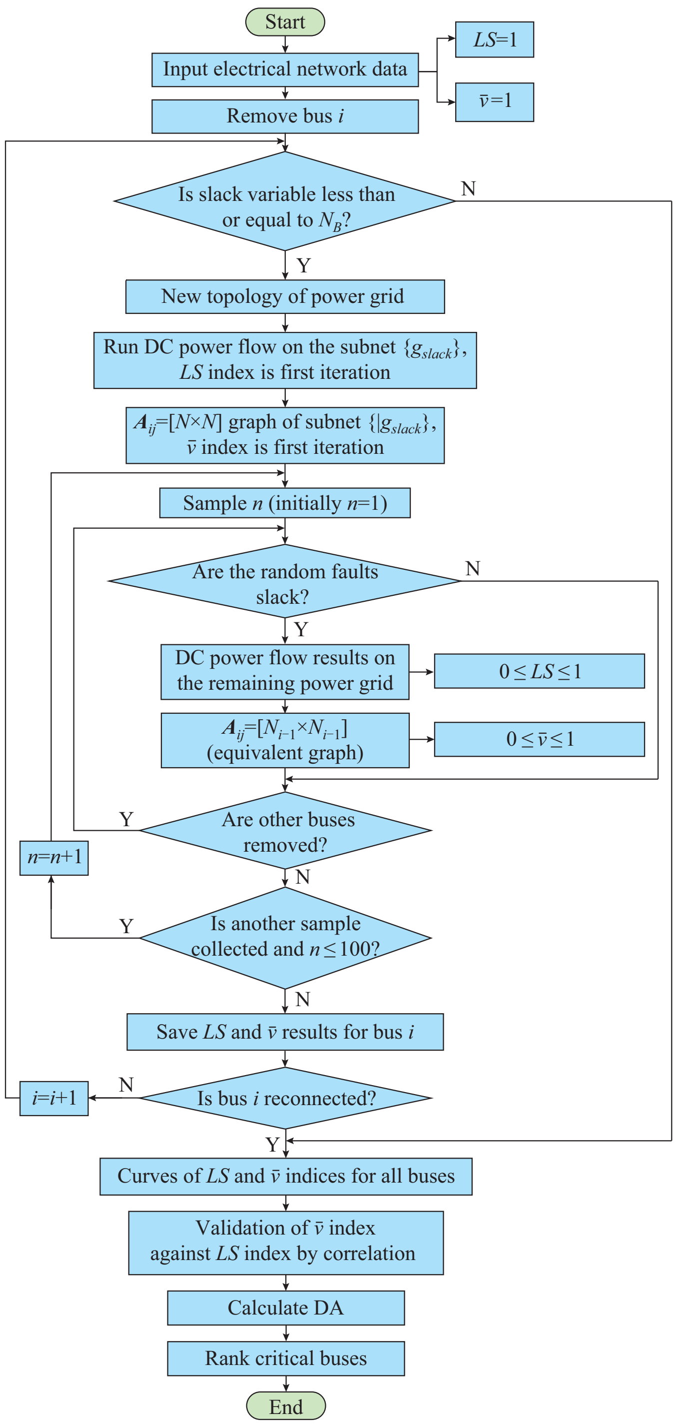

Fig. 2. Algorithm proposed to identify critical nodes in power systems.

Next, the procedure for identifying critical nodes is described in detail.

The first step of the algorithm in Fig. 2 is to collect the necessary data to simulate the critical infrastructure of electricity, assuming the models presented in Fig. 1. Both LS and $\bar{v}$ are initialized as 1.

The algorithm starts by removing the first electrical bus of the system. If this bus is equal to the slack bus, then the first electrical bus is reconnected, and the procedure is repeated with the next node of the network. In this case, the slack bus is not disconnected because it balances the power in the system.

Note that after a component is removed, a new topology is formed on the power system. The algorithm in Fig. 2 considers the subnetworks that are generated as a result of the previous event. Then, the island with the slack generator is selected, and the problem of DC load flow is solved. In this work, the DC model is used because only the active power injected into the network is intended to be measured. As a note, variations in voltage and frequency could occur during the process of network decomposition. However, these parameters are not relevant in the proposed methodology, since we consider only the structural performance of the network. Thus, once the evaluation of power flow is completed, the power produced by the slack generator is used to calculate LS with (1). In parallel, the adjacency matrix $\boldsymbol{A}_{ij}$ is built, which represents the equivalent graph of the selected subnetwork. Similarly, $\bar{v}$ is estimated with (2).

In turn, the subnetwork that results from the first bus removed is selected as a candidate to be attacked by the random removal of nodes. According to the central limit theorem, a certain number of experiments are required to obtain an adequate statistical sample [61]. In this case, 100 samples are used on each initial candidate subnetwork. Henceforth, random nodes are eliminated except for the slack generator. Indicators of (1) and (2) are calculated iteratively in each disintegration step.

Once the desired number of trials is reached, the total set of disintegration results is averaged for each of LS and $\bar{v}$. The average obtained for both indicators is saved as correspondence to bus i. Consequently, the bus is reconnected and the procedure is repeated until all the nodes of the electrical network N_B have been evaluated.

Next, to evaluate each set of results and determine the ranking of critical buses, the algorithm in Fig. 2 initially determines the correlation between LS and $\bar{v}$ to validate the use of the statistical measure of the networks. Then, the damage area (DA) is calculated for each of the saved results in Section III. In this case, a low DA value indicates a high criticality level. Conversely, a high DA value indicates a low criticality level. Finally, according to the above considerations, the most critical buses of the electricity infrastructure are classified.

III. Case Study

In this study, an IEEE 118-bus test system is used to demonstrate the effectiveness of the proposed methodology [62]. Initially, the selected structural characteristics of the case study are detailed, and then the simulation results obtained from 118 different topologies are exposed. Subsequently, the correlation analysis between LS and $\bar{v}$ is presented, and the most critical buses of the system are reported by both DA for each cascading failure curve.

A. Topological Characteristic of Case Study

The nodal degree distribution allows to visualize the percentage of nodes in network $P(k)$ which has a certain number of connections k. Figure 3 shows the nodal degree distribution for the IEEE 118-bus test system [62].

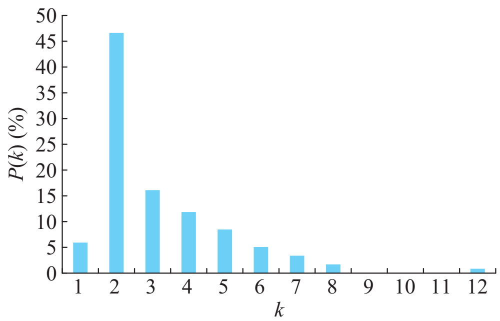

Fig. 3. Nodal degree distribution for case study.

Figure 3 shows that the test system has approximately 6% of the single-link nodes, which means that certain electrical substations remain connected by only one line to the system. In turn, more than 45% of the graph nodes have only two links, which indicates that most buses of the IEEE 118-bus test system have little connectivity with other infrastructure assets.

On the other hand, when the node percentages with connections from $k = 3$ to $k = 11$ are compared, a clear decrease in connectivity of the graph components is observed, and when $k = 12$, approximately 1% of the buses have the maximum connectivity degree. Specifically, a larger number of k links correspond to a lower number of components with high connectivity. The latter reflects a characteristic studied previously to identify this type of graph as a scale-free network [1], [55].

These networks are useful because they can be used to carry out vulnerability studies and allow a characterization of basic resilience properties against random events [63]. Thus, critical nodes are identified from the perspective of random errors. Note that strongly-connected nodes can be important network assets and their losses or destructions may have severe consequences in system operation.

Table I summarizes other structural characteristics of the case study for an IEEE 118-bus test system. The IEEE 118-bus test system consists of 118 nodes V and 186 links E, with an average connection degree $\bar{k}$ of 3.034. This power system has a node with 12 links of maximum nodal degree $k_{\max}$, which makes it a vital component for the infrastructure operation. In addition, d and $\bar{l}$ are much larger than the initial geodesic efficiency $\bar{e}$ of the network, potentially producing severe problems of congested power flows that result from losing a component of the power system.

TABLE I
TOPOLOGICAL CHARACTERISTICS FOR CASE STUDY

Parameter	Value
V	118
E	186
$\bar{k}$	3.034
$k_{\max}$	12
d	14
$\bar{e}$	0.214
$\bar{l}$	6.309

The use of these statistical measures provides an initial perspective of the network performance, which is always necessary to consider when carrying out vulnerability studies or identification of critical components.

B. Simulation Results

We apply the algorithm proposed in Fig. 2 for the identification of critical components. Figure 4 presents the impact on the power supply to the power system through LS and $\bar{v}$, measured according to a certain number of nodes removed from the network f. Each curve represents the average of 100 disintegration simulations of 118 different topologies. Note that Fig. 4 represents only the cascading failure curves corresponding to the cases of slower (node 4) and faster (node 80) disintegration. The remaining 116 cascading failure curves appear between the lower and upper curves of Fig. 4.

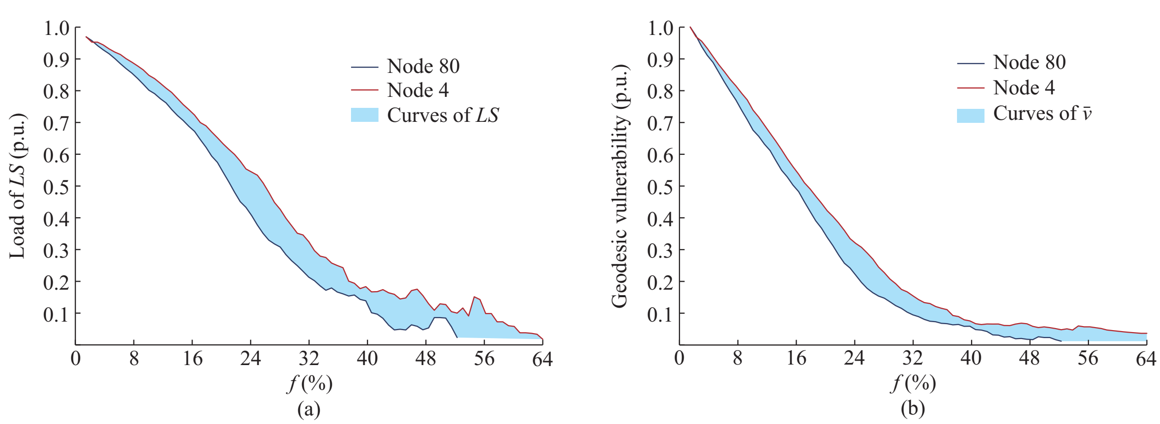

Fig. 4. Simulation results for case study. (a) Load flow index. (b) Graph index.

In the graphs, the values of LS and $\bar{v}$ are equal to 1 when all nodes and loads are initially connected. Then, as the network begins to decompose as a result of cascading disintegration, both indicators decrease until reaching a value equal to 0. In this last step, all nodes are isolated, and the electricity supply of the infrastructure has been interrupted.

1) LS

Figure 4(a) shows that in all cases, once the traditional technique of power flow is applied, the total collapse of the topologies that results from the initial removal of bus i is produced after eliminating approximately 60% of the nodes.

In other words, the 118 test networks present similar behavior when the nodes located in different positions are disconnected, which implies that cascading events occur with similar disintegration characteristics in all cases.

In turn, the case results show that although all the topologies reach the same final decomposition value, some topologies show a greater impact on the energy supply to the system for various partial fractions of eliminated nodes f. For example, LS curve for the topology in which node 80 is removed always has LS values below those of the other system assets. The LS curve for the topology in which node 4 is disconnected turns out to lie above the other curves of cascading events, which indicates a disintegration of the electrical network with less interruption of the energy supplied.

LS used in this work is very useful to visualize the effects of random events on the topologies of power systems. Furthermore, the large number of simulations performed on each test network allows a more precise estimation of the operation behavior for each of the topologies of electrical infrastructure.

We consider that this indicator provides a technical perspective of the conditions faced by the electrical networks. Therefore, the indicator allows the most critical buses to be identified under certain conditions.

2) $\bar{v}$

Figure 4(a) reports the results of $\bar{v}$ for each of the 118 topologies of the IEEE 118-bus test system. In this case, the results obtained with LS are compared to determining its possible utility.

Figure 4(a) shows that the values of $\bar{v}$ gradually decrease for each of the nodes. Identical to LS, only 60% of the nodes need to be removed to collapse the systems. Comparing the graphs, it is clear that the statistical measure of $\bar{v}$ has a behavior similar to that of LS. Therefore, the conclusions obtained in the previous subsection are also achieved by applying the complex network theory.

The results of the 118 topologies show that node 80 is the most critical and node 4 is one of the most robust. These results again confirm the results of LS.

C. Correlation Between LS and $\bar{v}$

One of the objectives of this paper is to mathematically validate the results obtained with $\bar{v}$ in comparison with the classical approach of power flow load shedding. However, the graphic representation in Fig. 4 is not sufficient to determine the level of correlation between both sets of results. Therefore, to achieve the research objective, the Pearson correlation coefficient is used to determine if there is a correlation between the results of $\bar{v}$ and LS [64]. The existence of this correlation validates $\bar{v}$ as an adequate indicator to identify the critical buses of the power system.

The Pearson correlation coefficient is calculated as:

$$\rho_i = \frac{\sigma(\bar{v}_i, LS_i)}{\sigma_{\bar{v}_i}\sigma_{LS_i}} \tag{3}$$

where ρ_i is the Pearson correlation coefficient between the results of node i; $\sigma\left(\bar{v}_i, LS_i\right)$ is the covariance between the results of $\bar{v}$ and LS for node i; $\sigma_{\bar{v}_i}$ is the standard deviation of $\bar{v}$ results for node i; and σ_{LS_i} is the standard deviation of LS results for node i.

The value of the correlation index varies in the interval between +1 and −1, where a value of +1 indicates a perfect positive correlation, a value of 0 means no linear correlation, and a value of −1 shows a perfect negative correlation [64]. Figure 5 shows the Pearson correlations for the 118 topologies calculated in Fig. 4. All topologies have correlations ρ_i greater than 0.96, which implies a positive linear relationship between the results of $\bar{v}$ and LS. We conclude that the statistical measurement of $\bar{v}$ index is useful for calculating the power supplied to the electrical network in a cascading failure process. In the end, the statistical result confirms the similarity of the curves shown in Figs. 4(a) and (b).

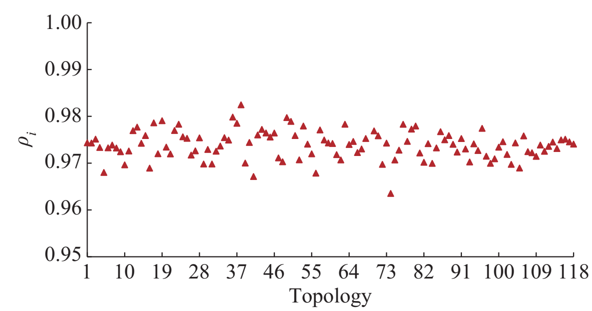

Fig. 5. Pearson correlation coefficients between $\bar{v}$ and LS for 118 topologies.

Thus, $\bar{v}$ has adequate accuracy relative to the classic power flow approach. However, this indicator only uses the graph connectivity and does not require technical information, which grants it a great advantage over LS. Therefore, $\bar{v}$ can be used to compare different topologies of power networks and determine which is the most vulnerable.

Table II shows the computational time (100 samples for each of the 118 topologies) of the algorithm of Fig. 2, where DC power flows are performed by using $\bar{v}$ alternatively. And it is carried on personal computer with Intel® Core™ i7 CPU 3.40 GHz and 32 GB of RAM.

TABLE II
COMPUTATIONAL TIME OF ALGORITHM OF FIG. 2

Index	Computational time (min)
LS	2850
$\bar{v}$	165

From the perspective of computation, it is observed that the statistical graph index is more efficient than the DC power flow on the power system because the computational time is reduced by more than 94%.

The importance of the proposed $\bar{v}$ is that it can be used to evaluate the robustness of electrical infrastructures without requiring electrical parameters, and its implementation may be useful for helping system operators identify critical buses.

D. Identification of Critical Components

$\bar{v}$ has shown a suitably linear relationship with the traditional power flow approach (*LS*). Therefore, it is possible to replace the latter with the statistical graph index. Thus, we propose to use the results shown in Fig. 4(a) to identify the critical buses of the power systems.

Since it is not visually possible to precisely plot the performance of each disintegration event shown in Fig. 4(a), the calculation of DA in the flow diagram of Fig. 2 for each set of results is proposed to determine the damage caused by the elimination of a certain asset in the electricity network. The strategy is carried out in the algorithm of Fig. 2 as follows.

Step 1: determine the equations that represent each of the disintegration curves of Fig. 4(a).

Step 2: calculate the integral of each equation in *Step 1* which is used as the limit of the fraction of nodes removed f for each curve.

Step 3: sort the results obtained in *Step 2* from lower to higher.

Consider that $\bar{v}$ is initially equal to 1 when the entire power system is connected. As the network is disintegrating, $\bar{v}$ tends to be 0. Therefore, it is assumed that a lower DA value represents greater damage to the electrical infrastructure because lower values are associated with the disintegration. In turn, a higher DA value represents less damage to the power system. *Steps 1* to *3* are detailly shown in Fig. 6.

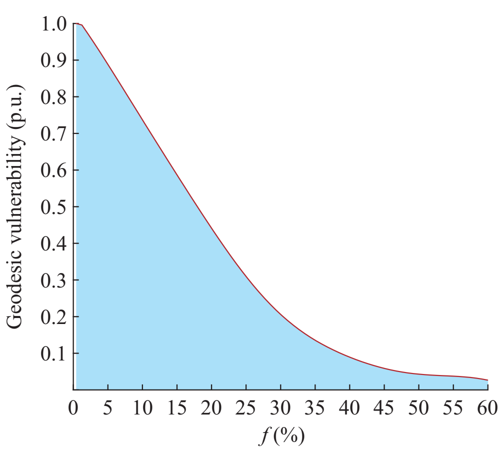

Fig. 6. Calculation of DA for cascading failure curves.

Table III reports the critical buses of the IEEE 118-bus test system using the strategy mentioned above. Note that without considering slack node 69, components 80, 49 and 77 are the most critical to the system under study. Furthermore, the buses in Table III are listed in the order of criticality. These are the nodes with a high number of connections (higher nodal degree of the system) or with a high connected electrical load.

TABLE III
BUS CRITICALITY ORDER OF IEEE 118-BUS TEST SYSTEM ACCORDING TO DA OF $\bar{v}$

Case study	Critical node
IEEE 118-bus test system	69 (slack generator), 80, 49, 77, 92, 8, 17, 89, 9, 24, 96, 116, 82, 19, 94, 37, 71, 106, 23, 115, 85, 38, 30, 46, 75, 70, 88, 56, 99, 68, 103, 72, 76, 78, 25, 40, 83, 12, 101, 114, 86, 61, 62, 34, 44, 32, 59, 51, 104, 87, 15, 112, 27, 113, 105, 81, 65, 74, 90, 29, 109, 50, 31, 26, 91, 52, 21, 45, 16, 98, 97, 93, 107, 111, 117, 55, 22, 43, 64, 73, 53, 63, 67, 110, 1, 66, 14, 13, 3, 79, 47, 118, 28, 36, 35, 102, 58, 7, 108, 84, 60, 48, 100, 11, 20, 95, 54, 39, 33, 57, 41, 18, 42, 5, 10, 6, 2, 4

Regarding the less critical buses in Table III, the cascading failure as a consequence of the disintegration of the network after the elimination of node 4 is the most favorable case.

IV. CONCLUSION

This paper proposes a methodology to identify the critical buses of power grids by using $\bar{v}$. To justify the scope of the results of the topological indicator, a comparative analysis versus the traditional power flow load shedding approach is carried out. The high correlation between the indices is validated mathematically. It allows the replacement of power flow routines that use electrical parameters and demands a high computational cost for a graph index which requires system connectivity and consumes less computational time. The results of the topological indicator are adequate for both the analysis of electricity infrastructure topologies when an asset is eliminated and the evaluation of each subsequent cascading failure. Future research will focus on the islands formed during the execution of the algorithm, the selection of new slack generators in the process of systemic disintegration and the integration of knowledge from the network operators.

REFERENCES

[1] R. Albert and A. L. Barabási, "Statistical mechanics of complex networks," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 47-97, Jan. 2002.

[2] X. Zhang and C. K. Tse, "Assessment of robustness of power systems from a network perspective," *IEEE Journal on Emerging and Selected Topics in Circuits Systems*, vol. 5, no. 3, pp. 456-464, Sept. 2015.

[3] U.S.-Canada Power System Outage Task Force. (2004, Apr.). Final report on the August 14, 2003 blackout in the United States and Canada: causes and recommentations. [Online]. Available: http://researchgate.net/publication/260082764

[4] J. M. Ordacgi-Filho. (2015, Oct.). Brazilian blackout 2009: blackout watch. [Online]. Available: http://www.pacw.org/fileadmin/doc/MarchIssue2010/Brazilian_Blackout_march_2010.pdf

[5] B. Sweet, "A post-mortem on India's blackout," *IEEE Spectrum*, Aug. 2012.

[6] X. Chen, K. Sun, Y. Cao *et al.*, "Identification of vulnerable lines in power grid based on complex network theory," in *Proceedings of 2007 IEEE PES General Meeting*, Jilin, China, Jun. 2007, pp. 1-6.

[7] C. Han, Y. Zhao, Z. Lin *et al.*, "Critical lines identification for skeleton-network of power systems under extreme weather conditions based on the modified VIKOR method," *Energies*, vol. 11, no. 6, p. 1355,

May 2018.

[8] D. T. Nguyen, Y. Shen, and M. T. Thai, "Detecting critical nodes in interdependent power networks for vulnerability assessment," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 151-159, Mar. 2013.

[9] V. Venkateswaran and W. Bennette, "Critical node analysis (CNA) of electrical infrastructure networks," in *Proceedings of SPIE 9850, Machine Intelligence and Bio-inspired Computation: Theory and Applications X*, Nice, France, May 2016, pp. 1-15.

[10] A. Sen, A. Mazumder, J. Banerjee *et al*., "Identification of *K* most vulnerable nodes in multi-layered network using a new model of interdependency," in *Proceedings of 2014 IEEE Conference on Computer Communications Workshops*, Toronto, Canada, May 2014, pp. 831-836.

[11] A. M. L. Da Silva, J. L. Jardim, L. R. De Lima *et al*., "A method for ranking critical nodes in power networks including load uncertainties," *IEEE Transactions on Power Systems*, vol. 31, no. 2, pp. 1341-1349, Mar. 2016.

[12] Y. Li, D. Ma, H. Zhang *et al*., "Critical nodes identification of power systems based on controllability of complex networks," *Applied Science*, vol. 5, no. 3, pp. 622-636, Sept. 2015.

[13] A. Wang, Y. Luo, G. Tu *et al*., "Vulnerability assessment scheme for power system transmission networks based on the fault chain theory," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 442-450, Feb. 2011.

[14] B. Liu, Z. Li, X. Chen *et al*., "Recognition and vulnerability analysis of key nodes in power grid based on complex network centrality," *IEEE Transactions on Circuits Systems II Express Briefs*, vol. 65, no. 3, p. 1, Mar. 2018.

[15] Z. Wang, J. He, A. Nechifor *et al*., "Identification of critical transmission lines in complex power networks," *Energies*, vol. 10, no. 9, pp. 1-19, Aug. 2017.

[16] R. Fang, R. Shang, Y. Wang *et al*., "Identification of vulnerable lines in power grids with wind power integration based on a weighted entropy analysis method," *International Journal of Hydrogen Energy*, vol. 42, no. 31, pp. 20269-20276, Aug. 2017.

[17] H. Bai and S. Miao, "Hybrid flow betweenness approach for identification of vulnerable line in power system," *IET Generation*, *Transmission & Distribution*, vol. 9, no. 12, pp. 1324-1331, Aug. 2015.

[18] A. B. M. Nasiruzzaman and H. R. Pota, "Modified centrality measures of power grid to identify critical components: method, impact, and rank similarity," in *Proceedings of 2012 IEEE PES General Meeting*, San Diego, USA, Jun. 2012, pp. 1-8.

[19] A. B. M. Nasiruzzaman and H. R. Pota, "Critical node identification of smart power system using complex network framework based centrality approach," in *Proceedings of 2011 North American Power Symposium*, Boston, USA, Aug. 2011, pp. 1-6.

[20] Y. Koc, T. Verma, N. A. M. Araujo *et al*., "MATCASC: a tool to analyse cascading line outages in power grids," in *Proceedings of 2013 IEEE International Workshop on Intelligent Energy Systems*, Vienna, Austria, Jan. 2013, pp. 143-148.

[21] A. Dwivedi, X. Yu, and P. Sokolowski, "Identifying vulnerable lines in a power network using complex network theory," in *Proceedings of 2009 IEEE International Symposium on Industrial Electronics*, Seoul, South Korea, Aug. 2009, pp. 18-23.

[22] X. Wang, Y. Koç, R. E. Kooij *et al*., "A network approach for power grid robustness against cascading failures," in *Proceedings of 2015 7th International Workshop on Reliability Networks Design Model*, Munich, Germany, Nov. 2015, pp. 208-214.

[23] C. M. Schneider, A. A. Moreira, J. S. Andrade *et al*., "Mitigation of malicious attacks on networks," *Proceedings of the National Academy of Sciences*, vol. 108, no. 10, pp. 3838-3841, Mar. 2011.

[24] G. Chen, Z. Y. Dong, D. J. Hill *et al*., "An improved model for structural vulnerability analysis of power networks," *Physica A: Statistical Mechanics and Its Applications*, vol. 388, no. 19, pp. 4259-4266, Oct. 2009.

[25] A. S. Alayande and N. Nwulu, "A novel approach for the identification of critical nodes and transmission lines for mitigating voltage instability in power networks," *African Journal of Science, Technology, Innovation and Development*, vol. 11, no. 3, pp. 383-390, Apr. 2019.

[26] O. B. Adewuyi, M. S. S. Danish, A. M. Howlader *et al*., "Network structure-based critical bus identification for power system considering line voltage stability margin," *Journal of Power Energy Engineering*, vol. 6, no. 9, pp. 97-111, Sept. 2018.

[27] I. Adebayo, A. A. Jimoh, and A. Yusuff, "Voltage stability assessment and identification of important nodes in power transmission network through network response structural characteristics," *IET Generation, Transmission & Distribution*, vol. 11, no. 6, pp. 1398-1408, May 2017.

[28] J. Zhang, H. Xu, J. Yang *et al*., "Mining and ranking important nodes in complex network by K-shell and degree difference," in *Proceedings of International Conference of Pioneering Computer Scientist, Engineers and Educators*, Zhengzhou, China, Sept. 2018, pp. 371-381.

[29] I. G. Adebayo, A. A. Jimoh, A. A. Yusuff *et al*., "Alternative method for the identification of critical nodes leading to voltage instability in a power system," *African Journal of Science, Technology, Innovation and Development*, vol. 10, no. 3, pp. 323-333, May 2018.

[30] A. S. Alayande, A. A. Jimoh, and A. A. Yusuff, "Identification of critical buses and weak transmission lines using inherent structural characteristics theory," in *Proceedings of 2015 IEEE PES Asia-Pacific Power and Energy Engineering Conference*, Brisbane, Australia, Jan. 2016, pp. 1-5.

[31] C. W. Ten, A. Ginter, and R. Bulbul, "Cyber-based contingency analysis," *IEEE Transactions on Power Systems*, vol. 31, no. 4, pp. 3040-3050, Jul. 2016.

[32] J. Guo, Y. Han, C. Guo *et al*., "Modeling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties," *Energies*, vol. 10, no. 1, pp. 1-21, Jan. 2017.

[33] S. Paul and Z. Ni, "Vulnerability analysis for simultaneous attack in smart grid security," in *Proceedings of 2017 IEEE PES Innovative Smart Grid Technologies Conference*, Washington DC, USA, Oct. 2017, pp. 1-5.

[34] H. Song, R. D. Dosano, and B. Lee, "Power grid node and line delta centrality measures for selection of critical lines in terms of blackouts with cascading failures," *International Journal of Innovation Computing, Information and Control*, vol. 7, no. 3, pp. 1321-1330, Mar. 2011.

[35] K. Wang, B. H. Zhang, Z. Zhang *et al*., "An electrical betweenness approach for vulnerability assessment of power grids considering the capacity of generators and load," *Physica A: Statistical Mechanics and Its Applications*, vol. 390, no. 23-24, pp. 4692-4701, Nov. 2011.

[36] A. M. Amani, M. Jalili, X. Yu *et al*., "Finding the most influential nodes in pinning controllability of complex networks," *IEEE Transactions on Circuits Systems II Express and Briefs*, vol. 64, no. 6, pp. 685-689, May 2017.

[37] X. Bai, D. Liu, J. Tan *et al*., "Dynamic identification of critical nodes and regions in power grid based on spatio-temporal attribute fusion of voltage trajectory," *Energies*, vol. 12, no. 5, p. 780, Feb. 2019.

[38] U. Nakarmi and M. Rahnamay-Naeini, "Analyzing power grids' cascading failures and critical components using interaction graphs," in *Proceedings of 2018 IEEE PES General Meeting*, Portland, USA, Nov. 2018, pp. 1-5.

[39] U. Nakarmi, M. Rahnamay-Naeini, and H. Khamfroush, "Critical component analysis in cascading failures for power grids using community structures in interaction graphs," *IEEE Transactions on Network Science Engineering*. DOI:10.1109/TNSE.2019.2904008

[40] J. Gao, X. Liu, D. Li *et al*., "Recent progress on the resilience of complex networks," *Energies*, vol. 8, no. 10, pp. 12187-12210, Oct. 2015.

[41] Y. P. Fang, G. Sansavini, and E. Zio, "An optimization-based framework for the identification of vulnerabilities in electric power grids exposed to natural hazards," *Risk Analysis*, vol. 39, no. 9, pp. 1949-1969, Sept. 2019.

[42] S. Amini, F. Pasqualetti, M. Abbaszadeh *et al*., "Hierarchical location identification of destabilizing faults and attacks in power systems: a frequency-domain approach," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2036-2045, Mar. 2019.

[43] J. E. Anderson and A. Chakrabortty, "PMU placement for dynamic equivalencing of power systems under flow observability constraints," *Electric Power Systems Research*, vol. 106, pp. 51-61, Jan. 2014.

[44] M. Randhawa, B. Sapkota, V. Vittal *et al*., "Voltage stability assessment of a large power system," in *Proceedings of 2008 IEEE PES General Meeting*, Portland, USA, Aug. 2008, pp. 1-7.

[45] F. Lian, A. Chakrabortty, and A. Duel-Hallen, "Game-theoretic multiagent control and network cost allocation under communication constraints," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 2, pp. 330-340, Feb. 2017.

[46] A. Taha, M. Bazrafshan, S. A. Nugroho *et al*., "Robust control for renewable-integrated power networks considering input bound constraints and worst-case uncertainty measure," *IEEE Transactions on Control Network Systems*, vol. 6, no. 3, pp. 1210-1222, Jul. 2019.

[47] S. Adhvaryyu, C. Mukherjee, and D. Seri, "Security constrained optimal power flow with optimally allocated UPFC based on technical and economic criteria," in *Proceedings of 2017 International Conference on Computer, Electrical & Communication Engineering*, Kolkata, India, Nov. 2018, pp. 1-5.

[48] D. Sen, M. Gupta, M. Shegaonkar *et al*., "Optimal location determination of UPFC based on techno-economic criteria and security constraints," in *Proceedings of 2018 International Conference on Power*

Energy, Environment and Intelligent Control, Greater Noida, India, Mar. 2019, pp. 534-539.

[49] L. K. Gallos, R. Cohen, P. Argyrakis *et al*., "Stability and topology of scale-free networks under attack and defense strategies," *Physics Review Letter*, vol. 94, no. 18, pp. 1-4, May 2005.

[50] J. V. Milanovic and W. Zhu, "Modeling of interconnected critical infrastructure systems using complex network theory," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4637-4648, Sept. 2018.

[51] S. S. Ahmed, N. C. Sarker, A. B. Khairuddin *et al*., "A scheme for controlled islanding to prevent subsequent blackout," *IEEE Transactions on Power Systems*, vol. 18, no. 1, pp. 136-143, Feb. 2003.

[52] B. Yang, V. Vittal, and G. T. Heydt, "Slow-coherency-based controlled islanding – a demonstration of the approach on the August 14, 2003 blackout scenario," *IEEE Transactions on Power Systems*, vol. 21, no. 4, pp. 1840-1847, Oct. 2006.

[53] S. Kamali and T. Amraee, "Blackout prediction in interconnected electric energy systems considering generation re-dispatch and energy curtailment," *Applied Energy*, vol. 187, pp. 50-61, Feb. 2017.

[54] S. Kamali, T. Amraee, and F. Capitanescu, "Controlled network splitting considering transient stability constraints," *IET Generation Transmission & Distribution*, vol. 12, no. 21, pp. 5639-5648, Nov. 2018.

[55] M. E. J. Newman, "The structure and function of complex networks," *Siam Review*, vol. 45, no. 2, pp. 167-256, Mar. 2003.

[56] V. Ajjarapu and C. Christy, "The continuation power flow: a tool for steady state voltage stability analysis," *IEEE Transactions on Power Systems*, vol. 7, no. 1, pp. 416-423, Feb. 1992.

[57] A. M. Haidar, A. Mohamed, and A. Hussain, "Vulnerability assessment of a large sized power system considering a new index based on power system loss," *European Journal of Science Research*, vol. 17, no. 1, pp. 61-72, Apr. 2007.

[58] J. Reichardt, *Structure in Complex Networks*. Heidelberg: Springer, Nov. 2009.

[59] Y. Koç, M. Warnier, P. Van Mieghem *et al*., "The impact of the topology on cascading failures in a power grid model," *Physica A: Statistical Mechanics and Its Applications*, vol. 402, pp. 169-179, May 2014.

[60] J. Johansson, "Risk and vulnerability analysis of interdependent technical infrastructures: addressing socio-technical systems," Ph.D. dissertation, Lund University, Lund, Sweden, Mar. 2010.

[61] J. E. Gentle, *Theory of Statistics*. New York: Springer, 2013.

[62] IEEE. (2018, Jul.). IEEE power systems test case. [Online]. Available: https://www2.ee.washington.edu/research/pstca/

[63] B. Bollobás and O. Riordan, "Robustness and vulnerability of scale-free random graphs," *Internet Mathematics*, vol. 1, no. 1, pp. 1-35, Jan. 2003.

[64] D. R. Anderson, D. J. Sweeney, and T. A. Williams, *Essentials of Statistics for Business and Economics*. Boston: South-Western, 2011.

Jesus Beyza received the bachelor's degree in electromechanical engineering from Instituto Tecnologico de la Costa Grande, la Costa Grande, Mexico, in 2014, and the M.Sc. degree in electrical engineering from Instituto Tecnologico de Morelia, Morelia, Mexico, in 2017. In 2014, he received the National Award of National Association of Schools of Engineering (ANFEI). He is currently pursuing a Ph.D. degree. in electrical engineering. His research interests include power system protection and control, power system reliability and resiliency, and smart electricity grid applications.

Eduardo Garcia-Paricio received the bachelor's degree in industrial engineering in 1994, and a Ph.D. degree in electrical engineering in 2015, from the Universidad de Zaragoza, Zaragoza, Spain. He is currently an Associate Professor of Department of Electrical Engineering at Universidad de Zaragoza. His areas of interest are renewable energy and energy efficiency.

Hector F. Ruiz Paredes received the bachelor's degree in electrical engineering from the Instituto Tecnologico de Morelia, Morelia, Mexico, in 1976, the M.Sc. degree in electrical engineering from the Instituto Tecnologico de Estudios Superiores de Monterrey (ITESM), Monterrey, Mexico, in 1977, and the Ph.D. degree in electrical engineering from the University of Manchester, Manchester, UK, in 1992. He was the founder of the "Graduate Program and Research in Electrical Engineering" from the Instituto Tecnologico de Morelia, Mexico, where he is currently a Professor. His areas of interest are power and distribution systems.

Jose M. Yusta received the bachelor's degree in industrial engineering in 1994, and a Ph.D. degree in electrical engineering in 2000, from the Universidad de Zaragoza, Zaragoza, Spain. He is currently a Professor of Department of Electrical Engineering at Universidad de Zaragoza. From 2004 to 2007, he was vice-dean of Faculty of Engineering from Universidad de Zaragoza. His areas of interest are electricity markets and vulnerability analysis of critical infrastructure.