ECCOMAS Congress 2016
VII European Congress on Computational Methods in Applied Sciences and Engineering
M. Papadrakakis, V. Papadopoulos, G. Stefanou, V. Plevris (eds.)
Crete Island, Greece, 5–10 June 2016

POWER GRID ROBUSTNESS TO SEVERE FAILURES: TOPOLOGICAL AND FLOW BASED METRICS COMPARISON

Roberto Rocchetta[1],**Edoardo Patelli**[1]

[1]Institute of Risk and Uncertainty, University of Liverpool
L69 7ZF, Liverpool, United Kingdom
e-mail: {Roberto.Rocchetta,Edoardo.Patelli}@liverpool.ac.uk

Keywords: Power Grid Robustness, Vulnerability Metrics, Spectral Graph Analysis, Cascading Failures, Uncertainty.

Abstract. *Power grids are generally regarded as a very reliable systems, nevertheless outages and electricity shortfalls are common events. Severe accidents have the potential to produce significant social and economic consequences, hence it is important to reduce their likelihood by assuring safe operations robust topologies. Grid safety relies on accurate vulnerability measures, control schemes and good quality information, for instance during power network operations, contingency analysis is used to constrain the network to secure operative states with respect to predefined failures (e.g. list of single component failures). In order to better understand the power network weakness and strengths a variety of robustness metrics have been introduced in literature. In this work power network vulnerabilities to failure events are analysed and the most relevant outages have been ranked using different metrics, i.e. topology-based, flow-based and hybrid metrics. Single line failures (N-1 contingencies) have been investigated and sources of uncertainty such as variability in the power demand and imprecision in the line parameters have considered in all the phases of the calculation. The assumption underpinning the methodologies and results are discussed. The different metrics have been compared before and after the uncertainty quantification. A modified version of the IEEE 118 bus power network has been selected as representative case study. Through the metrics comparison it has been possible to point out interesting aspects of the different robustness indexes and better consideration of uncertainties in the calculations.*

1 INTRODUCTION

Power Grid has been historically developed to distribute electric power from large size isolated power plants to the various end-user loads (e.g. industry or residences) by means of power transmission and distribution networks. The distribution grids topologies were usually designed in radial fashion to comply with the needs of a simple one-way flow of electricity, i.e. from the main grid to the local users.

In the last decades, the power grid traditional paradigm has deeply changed. Distribution networks are getting more active in the power production due to increasing share of distributed renewable generators (e.g. micro wind turbines, photovoltaic panels)[1]. Non-classical design and non-radial complex meshed topologies are likely to became more common in the future [2]. In this designs of increasing complexity, is important to understand the role played by variability in both power demand and power production sides and by imprecise knowledge of the network parameters. More specifically, allocation of renewable distributed generators are injecting considerable amount of uncertainty [3], making the system behaviour less deterministic and classical vulnerability assessment less reliable. Furthermore structural weaknesses have to be understood to provide more robust topologies and mitigate likelihood of unexpected hazardous scenarios.

The presented scenario highlights the need of develop improved frameworks for power grid vulnerability analysis (i.e. sophisticated uncertainty quantification techniques) as well as the need of define enhanced metric for the identification of operational and structural risks. Robustness of power networks is defined as the degree to witch the network is able to withstand an unexpected event without degradation in performance [4]. A closely related concept is the vulnerability, which is sometime regarded as lack of robustness. A wide range of indexes have been proposed in literature for their assessment, e.g. using realistic simulation of network response and power-flow solution ("power-flow-based metrics").

Vulnerability assessments for power girds were also based on topological analysis of networks, using techniques founded on complex network theory [5]. For these approaches, the vulnerability indexes have been computed using pure topological approaches (i.e. 'topology-based metrics') or enhanced by including electrical engineering concepts in the analysis (i.e. 'hybrid metrics'). The hybrid metrics have been introduced on the idea that pure topological approach may fail in exhaustive captivation of the electric networks complexity and criticality, see as example [6]. It is work remarking that a controversy still open centred on weather or not pure topological approaches and hybrid approaches are capable of fully capture vulnerabilities in power girds [5]. Few examples of recently applied metrics are the effective resistance ($R_{\mathcal{G}}$), network spectral radius ($\rho_{\mathcal{G}}$), algebraic connectivity ($\Lambda_{\mathcal{G}}$) and extended betweenness ($\mathcal{B}_e$). For further details about these metrics the readers are reminded to [7], [8] or [9].

M. Ouyang et al. [11] analysed correlation of six topology-based vulnerability metrics respect to single and multiple component failure. E. Bompard et al. [8] compared two hybrid metrics (i.e. extended betweenness and net-ability) by ranking components with respect to the system vulnerability. Recently, Lucas Cuadra et al. [5] reviewed power grid robustness metrics computed adopting complex network theory approaches.Concerning the power-flow-based metrics, quantity such as system cascading index (CEI), has been applied to estimate the degradation of performance, likelihood and extent of cascading failures [1]-[10].

To the Authors knowledge, further comparison between different metrics seems to be needed. In this survey, single line failures ($N-1$ contingencies) have been considered as threatening events. Sources of uncertainty due to imprecise knowledge of the network parameters and variability in the power demand have been accounted for. Their effects have been quantified in the vulnerability metrics and in the contingency ranking. In addition, different power-flow models (i.e. alternate current and direct current power-flows) have been compared in the results. The work aim is to better understand strength and limitations of the different metrics and explore their capability in ranking critical components and spot network strength and weaknesses.

The paper is structured as follows:
Power network modelling and a broad review power-flow solution methods is introduced in Section 2. Contingency analysis and uncertainty modelling are described in in Section 3. In Section 4 robustness and vulnerability concepts in power networks are discussed and the metrics used in the assessment defined. In Section 5 a case study and the results for different approaches are described. Some of the limitation faced and results are further discussed in Section 6 and Section 7 close the paper.

2 BACKGROUND AND POWER NETWORK MODELLING

A power network structure can be represented by an unweighed graph $\mathcal{G} = \{\mathcal{N}, \mathcal{L}\}$, where $\mathcal{N}$ is the set of network nodes (or busses) and $\mathcal{L}$ is the set of links (branches or feeders). The topology of the graph is identified by a squared symmetric matrix called adjacency matrix A, which elements $a_{i,j}$ are equal 1 if the node i is linked to the node j or 0 if no direct link exists. Links can be associated to some measure of interest (e.g. length, traffic, power flow, line resistance, etc.) and the adjacency matrix rewrite in its weighted form W, where the matrix elements $w_{i,j}$ are the weights of the links between nodes i and j and 0 if not linked.

Spectral graph theory is used analyse spectral graph proprieties of networks such as its eigenvalues eigenvectors. The Laplacian L of the adjacency matrix A is defined as [12]:

$$L_A = D_A - A \tag{1}$$

where A is the adjacency matrix and D_A is the diagonal matrix of degrees for A. The matrix L can be computed using the weighed adjacency matrix W (i.e. including electrical concepts such as susceptances). Spectral proprieties of graph $\mathcal{G}$ bears valuable information about the network the graph represent and some eigenvalues can be associated to its robustness [13]. Further details are going to be discussed in Section 4.

AC and DC Power Flow

Power flow methods are commonly used to solve problem in power grid analysis, as example the energy dispatch problem, i.e. optimal schedule of power production, or security constrained optimal power scheduling. Different solvers are founded on stronger or weaker assumptions and alternating current (AC) and direct current (DC) approaches are widely applied.
The AC power flow is a non linear solver accounting both active and reactive power flows without neglecting loses. In the AC formulation the active and reactive nodal equations are as follow [14]:

$$P_k = \sum_{i}^{N} |V_i||V_k|[G_{i,k}cos(\theta_{i,k}) + B_{i,k}sin(\theta_{i,k})] \tag{2}$$

$$Q_k = \sum_{i}^{N} |V_i||V_k|[G_{i,k}sin(\theta_{i,k}) - B_{i,k}cos(\theta_{i,k})] \tag{3}$$

where P_k and Q_k are active and reactive power injected in the node k, respectively, $|V_i|$ is the voltage magnitude of node i and $\theta_{i,j}$ is the voltage angle difference between node i and k. The elements $G_{i,k}$ and $B_{i,k}$ are the conductance and susceptance of the link connecting node i and k, respectively.The Equations 2-3 are solved for each $k \in \mathcal{N}$ by some iterative techniques (e.g. Newton-Raphson method) although convergence is not always assured.

The DC power flow is a linear approximation of the AC power flow which account for just active power flows, neglect power loses and reactive power management. It has been widely used to alleviate the computational cost of numerically intensive codes (e.g. reliability based designs or robust optimizations) and it has always a feasible solution. It has been adopted in transmission network analysis [14] but can be found also in distribution systems analysis [15]. The DC power flow formulation can be written as follows [14]:

$$P_k = \sum_{i}^{N} |V_i||V_k|B_{i,k}sin(\theta_{i,k}) \approx \sum_{i}^{N} B_{i,k}\theta_{i,k} \tag{4}$$

were the equation 4 is obtained under the following DC power flow assumptions:

- Flat voltage profile $|V_i| = 1\ p.u.\ \forall\ i \in \mathcal{N}$
- Small voltage angle differences$sin(\theta_{i,k}) \approx \theta_{i,k}$;
- $R \ll X$ negligible resistance;

It is worth remarking that DC model although useful in reducing computational time, might result in a poor approximation [14]. In order to obtain good quality results, grid voltage profile should be as flat as possible and ratio X/R relatively high. This means that the quality of the DC solution is system dependent and operative state dependent, hence its validity should be carefully assessed before use. The vast majority of topology-based metrics when enhanced by using electrical concepts made use of the DC assumptions [5]. Following the consideration made, the AC power flow is going to be considered as baseline method for comparison with DC power flow solutions.

3 CONTINGENCIES ANALYSIS AND UNCERTAINTY

Contingency Selection

A contingency in power networks is defined as the unexpected failure of one of its components (e.g. links, nodes, generators, transformers) [1]. Contingency analysis is commonly used to constrain the network to safe operational states if a contingency occurs. Generally speaking, even if the network has modest size (e.g. small distribution grid), a complete analysis of all possible failures is infeasible. An exhaustive contingency list will has to include $\sum_{k=1}^{N} N!/k!(N-k)!$ failures, where k is the number of failed components. Consider as example a very small network of just 50 components, exhaustive list include 50 single component failures (i.e. $N-1$

contingencies), 4900 $N-2$ contingencies, 705600 $N-3$ contingencies, more than 1.32x10^8 $N-4$ contingencies and so on. In power grid reliability and risk assessment, common practice consists in selecting a subset of the more threatening $N-1$ or $N-2$ contingencies based on expert opinion or some identification procedure [17]. Other works focused also on selecting the most threatening attack of link and node based on complex network measures such as maximum centrality [5]. In this work, the $N-1$ single line trips are analysed and the most threatening failures identified using different metrics. In addition, uncertainty analysis have been performed as described in the following subsection.

Uncertainty

Generally speaking, uncertainty can be separated in two groups, the so called aleatory and epistemic uncertainties [18]. The aleatory is related to stochastic behaviours and randomness in events and variables. The epistemic is commonly related to lack of knowledge about a particular behaviour, imprecision in measurement and poorly designed models. Adequately model uncertainty is paramount to improve robustness of the analysis accounting for both lack of information and inherent randomness (e.g. environmental conditions, future power demand, power produced by renewable generators, etc.). In the power grid context many of the sources of uncertainties which might be relevant for the analysis. Among the others, some of the well-recognized sources of variability are electricity price volatility, load power demand and environmental variability, model assumption (e.g. DC or AC power flow, contingency selection) and many others. The sources of uncertainty investigated (similarly to what done in [26]) are:

- Uncertainty in the line emergency rating which might be due to, e.g. neglected effect of ambient wind and temperature.
  The lack of precise knowledge on the emergency ratings of network lines have been modelled using uniform distributions around a given design value [26]. The uniform distribution has been used consistently with the principle of maximum entropy.

- Load demand uncertainty and variability.
  The aggregated load connected to a node can be described by a Normal distribution [1]. Its corresponding probability distribution function is the following:

  $$f(P_{L,i}) = \frac{1}{\sqrt{(2\pi)}\sigma_i} exp\left(-\frac{(P_{L,i}-\mu_i)}{2\sigma_i^2}\right) \tag{5}$$

  where $P_{L,i}$ is the load demand or power withdrawn form node i at hour of the day t, μ_i is the load mean value and σ_i is the standard deviation at node $i \in \mathcal{N}$. The parameter of the distribution can be estimated from historical records of load demand per node.

A simple Monte Carlo sampling procedure have been used to propagate uncertainty from the input to the output quantities of interest. Within each Monte Carlo run, sampling procedure (e.g. inverse transform sampling) is used to obtain a random realization for each uncertain parameter (nodal loads and line loading limits). The samples are forwarded to the system solver for vulnerability assessment. The algorithm allows obtaining a probabilistic description of the outputs variability, i.e. the output probability distribution functions with respect to the input uncertainties.

4 ROBUSTNESS AND VULNERABILITY METRICS

Robustness in power grid is defined as the degree to witch the network is able to withstand an unexpected event without degradation in performance [4]-[11]. Vulnerability is used to score low reliability power grids by assessing drops in performance metrics. The network vulnerability $\mathcal{V}(C_i)$ after the contingency (C_i) occurs can be quantified as follows [5]:

$$\mathcal{V}(C_i) = \frac{\mathcal{M} - \mathcal{M}(C_i)}{\mathcal{M}} \tag{6}$$

where $\mathcal{M}(C_i)$ is the network vulnerability metric after contingency Ci and $\mathcal{M}$ is the metric value for the undamaged network.

Power flow-based metrics

Flow-based indexes can be obtained by simulating network in normal and damaged states and using power flow solvers (e.g. DC or AC). In this work a cascading metric ($CEI(C_i)$) is obtained by simulating the outage with both AC power flow contingency analysis and its linear DC approximation. Generally speaking, a "cascading" is a sequential successions of dependent events [21]. In power system cascading analysis, many are the factors that can contributed or generate a sequence of failures. In a general way, line tripping can have two origins, one is load-driven when thermal expansion can result in the line dropping beneath its safety clearance, and one is load-independent such as mechanical failure [22]. In the adopted model, overload events are the one accounted for, the metric adopted to assess the cascading overload vulnerability is analogous to the one presented in [21]:

$$CEI(C_i) = \sum_{l \in \mathcal{L}} \mathcal{P}(C_l|C_i) SevOL_l(C_i) \tag{7}$$

where $\mathcal{P}(C_l|C_i)$ is the probability of secondary trip of line l after line i contingency occurs and $SevOL_l(C_i)$ is the severity function for line l overload if failure C_i occurs.

Severity functions are used to quantify the extent of the failure and different definitions are available [1]. The continuous severity function for overload is specifically defined for each circuit (distribution lines and transformers) and it measures the extent of violation in terms of excessive power flow as the percentage of rating:

$$PR_l = \frac{P_l}{P_{emerg,l}} \tag{8}$$

where P_l is the active power flowing in the line l and $P_{emerg,l}$ is the emergency rating of the line $l \in \mathcal{L}$. The expression for the continuous severity due to overload ($SevOL_l$) of a line l is findable in [21]. Continuous severity functions, if compared with discrete severity functions, have the advantage of providing non zero risk results for scenarios close to the performance limits, but not failure, which reflects the realistic sense that a near violation scenario is as a matter of fact risky. The probability of cascading trip of line k after an initiating contingency i can be expressed as in [10]:

$$\mathcal{P}(C_j|C_i) = \frac{P_j(C_i,\zeta) - P_{0,j}(\zeta)}{P_{trip,j}(C_i,\zeta) - P_{0,j}(\zeta)} \tag{9}$$

where $P_j(C_i, \zeta)$ is the post-contingency flow on circuit j given contingency i and operative-environmental condition ζ, $P_{trip,j}(C_i, \zeta)$ is defined as the flow leading to a certain trip of the line j (assumed to be 125% of its maximum capacity) and $P_{0,j}(\zeta)$ is the pre-contingency flow in the line j if condition ζ holds. Equation 9 is related to the fact that higher load levels and larger transients increases the likelihood of cascading event on circuit k after initiating event on circuit i. The probability $\mathcal{P}(C_j|C_i)$ is zero defined for $P_j(C_i, \zeta) \geq 0.9 P_{emerg,j}$.

Topology-based and hybrid metrics

Power network vulnerability is also assessed by pure topological analysis of the grid structure. These approach use unweighted adjacency matrix A to represent network structure, components are regarded as identical and no rough electrical concept is included in the analysis [5]. Similarly, hybrid metrics adopt complex network concepts but enhanced by inclusion of electrical engineering knowledge in the analysis. These often include concepts such as DC approximation and electrical concepts such as line emergency rating $P_{emerg,l}$ or link impedances. For these approaches the weighted adjacency matrix W is built using the matrix of susceptances $B_{i,k}$ [13]-[5]. The analysed metrics in this paper are: graph spectral radius, algebraic connectivity, effective graph resistance [13], graph global efficiency [28] and extended betweenness [8].

In spectral analysis of graphs, the largest eigenvalue of the adjacency matrix is known as graph spectral radius ($\rho_{\mathcal{G}}$). It has been used as indicator of robustness of networks against dynamic processes such as virus spreading or epidemic processes [20]. Few works attempted to relate spectral radius to the power grid vulnerability and relatively small values have been considered as indicator of robustness. In [13] it has been highlighted that spectral radius relates to process-based system transitions while algebraic connectivity to connectivity-based transitions.

Another important metrics obained through spectral analysis of the network graph is the second smallest eigenvalue of the Laplacian matrix L, also known as the algebraic connectivity ($\Lambda_{\mathcal{G}}$). The corresponding eigenvector is named the Fiedler vector which elements provide information about graph partitioning [9]. The metric $\Lambda_{\mathcal{G}}$ is used as indicator of the level of connection between nodes in a graph, higher values means that the network is more difficult to be partitioned in independent components. As example null value for $\Lambda_{\mathcal{G}}$ means that the network is disconnected. For these reasons the algebraic connectivity is regarded as a basic indication of network robustness level [19].

The effective graph resistance ($R_{\mathcal{G}}$) is an hybrid metric which have been sometimes related to the power grid vulnerability [13]. The effective resistance $R_{i,j}$ between a pair of nodes i and j is the potential difference between these nodes when a unit current is injected at node i and withdrawn at node j. In order to compute $R_{\mathcal{G}}$ information about the grid topology links parameters is needed. $R_{\mathcal{G}}$ can be obtained as follows:

$$R_{\mathcal{G}} = \sum_{i=1}^{N-1} \frac{1}{\mu_i} \tag{10}$$

were μ_i are the eigenvalues of the L obtained from the weighted adjacency matrix of susceptances.

Others vulnerability indicators commonly used in the power network topological analysis are global efficiency ($\mathcal{E}_{\mathcal{G}}$) and betweenness. The efficiency of a network is defined as the average of inverses of the distance for all nodes. The $\mathcal{E}_{\mathcal{G}}$ is defined as [28]:

$$\mathcal{E}_{\mathcal{G}} = \frac{1}{(N-1)N} \sum_{i,j \in \mathcal{N} i \neq j}^{N-1} \frac{1}{\mathcal{D}_{i,j}} \tag{11}$$

where N is the number of nodes in the network and $\mathcal{D}_{i,j}$ is the shortest path length between node i and j.

Betweenness has been recently used in [16] to identify most vulnerable lines in power systems. The extended betweenness ($T_e(l)$) has been introduced in [8] as fast metric to spot most critical lines in terms of system vulnerability. The metric $T_e(l)$ is based on both complex network and electrical concepts. For the line l is defined as follows [8]:

$$T_e(l) = max(|\sum_{g \in G} \sum_{d \in Ld} C_g^d f_l^{gd}|) \; l \in \mathcal{L} \tag{12}$$

where Gn and Ld are set of generation nodes and load nodes, C_g^d is the power transmission capacity from generator g to load d and f_l^{gd} is the linearised power flow sensitivity in the line l with respect to an injection in generation node g and withdraw in the demand node d. C_g^d and df_l^{gd} are computed as follows [8]:

$$f_l^{gd} = f_{lg} - f_{ld} \tag{13}$$

$$C_g^d = \min_{l \in \mathcal{L}} \left(\frac{P_{emerg,k}}{|f_l^{gd}|} \right) \tag{14}$$

where f_{ld} and f_{lg} are the elements of the power transfer distribution factors (PTDF) matrix corresponding to line l and demand node d and generation node g, respectively. The reader is reminded to [29] for further details on PTDF capability and calculation procedure.

5 CASE STUDY

The selected case study is a modified version of the IEEE 118 nodes test system. The network counts 118 nodes, 186 lines and 54 generators which makes it fairly complex and suitable for the analysis. Within the gird there are 55 PV nodes (i.e. generators nodes g) and 64 PQ nodes (i.e. load nodes d). The network model and data can be found between the MatPower software [24] or in reference [27]. Figure 1 displays the network structure and generators location. The original network data have been slightly modified in order to simulate a condition of higher stress for the network. The modified system includes an increment in the load demand of 30 $\%$ and $P_{emerg,l} \; \forall \; l \in \mathcal{L}$ reduced of 20$\%$.

Results power-flow-based metrics

The AC and its linearised version are used to simulate the network in normal and contingency states the cascading index CEI computed and line outages ranked. The analysis is performed as follows:

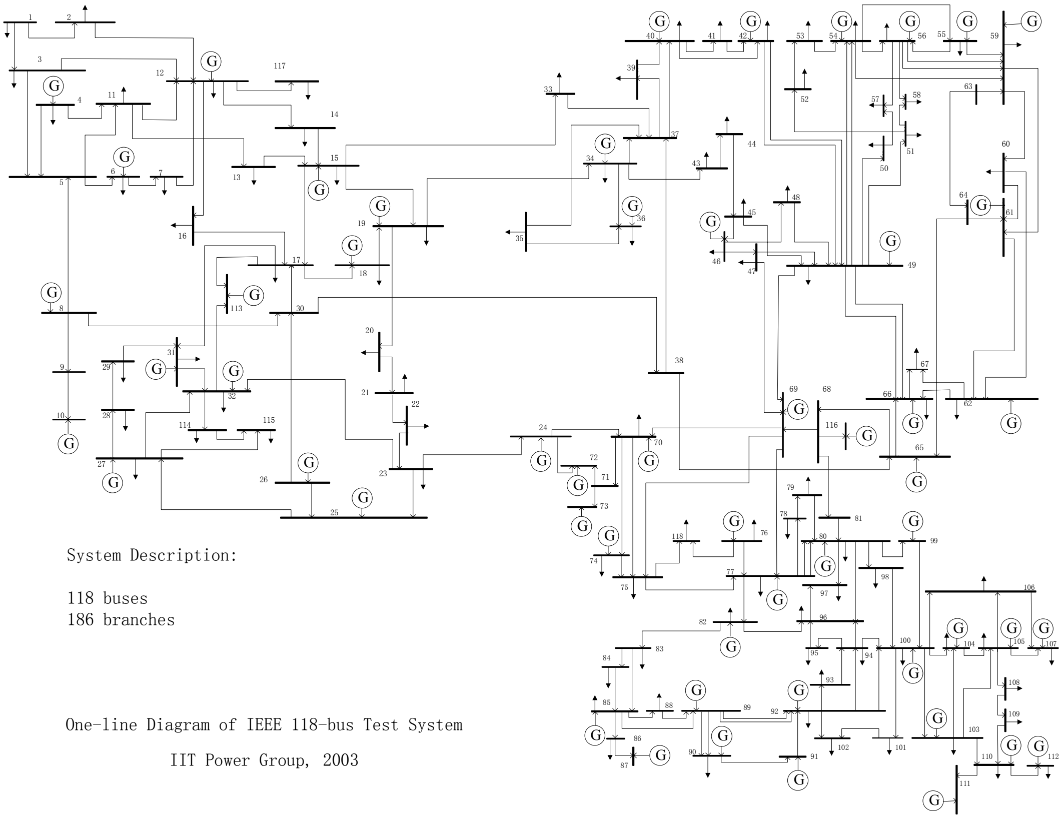

Figure 1: The IEEE 118 bus test system [27].

- First, AC or DC approach is selected and optimal power flow is solved. This solution is the optimal power production subject to line flow limits, generation constraints and load demanded.

- The contingency analysis is performed by removal of lines from the system. The AC or DC methods simulate the power flows redistribution in the branches given the optimal power scheduled.

- Finally, the $CEI(l)$ is computed for each contingency in equation 7. Line vulnerability are ranked and ordered based on the CEI value.

Figures 2 display a comparison between AC and DC solutions. Y-axis shows the normalized CEI results and the X-axis the line identification number (ID). It can be noticed that DC power flow overestimated the cascading index for some of the contingency listed (e.g. lines ID 141-150) and underestimate it for others e.g line ID 13, 43, 153 (l_{8-5}, l_{26-30}, l_{89-92}). This result is mainly due to the approximate percentage of rating PR_k obtained in the DC approach. Nevertheless, results are in relatively good agreement, therefore it might be argued that DC solutions approximate AC solutions fairly well in both undamaged and damaged network conditions. Table 1 displays the 10 most vulnerable lines in the system, with respect to the CEI metric. In both AC and DC flow-based approaches the ranking results are fairly similar and similar to previous studies, see as example [23]. The most threatening lines result to be l_{9-10}, l_{8-9}, l_{8-5}, l_{26-30} for both cases.

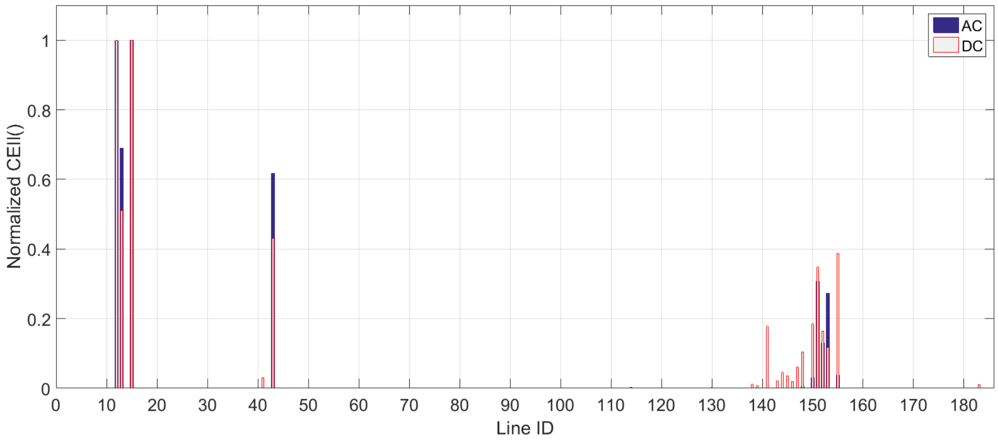

Figure 2: Normalized CEI results for N-1 line contingency. Comparison between AC solution and DC approximation solution.

Rank	CEI_{AC}		CEI_{DC}	
1	l_{9-10}	0.57365	l_{8-9}	0.5931
2	l_{8-9}	0.57246	l_{9-10}	0.5931
3	l_{8-5}	0.39562	l_{8-5}	0.3028
4	l_{26-30}	0.35366	l_{26-30}	0.2549
5	l_{89-90}	0.17620	l_{91-92}	0.2297
6	l_{89-92}	0.15594	l_{89-90}	0.2066
7	l_{89-91}	0.07426	l_{88-89}	0.1099
8	l_{91-92}	0.02133	l_{82-83}	0.1056
9	l_{88-89}	0.01678	l_{89-91}	0.0973
10	l_{85-89}	0.00246	l_{89-92}	0.0691

Table 1: Ten most vulnerable lines for the IEEE 118 bus system with respect to the normalized cascading index. The AC and DC ranking score comparison.

Uncertainty Quantification for the AC and DC Solutions

The AC and DC cascading indexes have been obtained by propagation of the uncertainty in the load and in the emergency ratings. In accordance with previous studies, the load demand $P_{L,i}$ $\forall i \in \mathcal{N}$ has been modelled as normal random variable distributed around mean μ_i and with σ_i equal to 10 $\%$ of μ_i. Uniform distributions are assumed to model lack of precision in the line maximum allowed flows. The upper and lower bounds have been set equal to 0.98 $\%$ and 1.02 $\%$ of the design values. A single loop Monte Carlo has been employed to sample input uncertainty and quantify its extent in the output. The number of MC samples for each uncertain variable have been set equal to 2x10^3, each run counts 64 samples of load demand $P_{L,d}$ and 185 samples of emergency rating $P_{emerg,l}$ one for each demand node and each line $\in \mathcal{G}$ in the network. Samples have been forwarded to the AC and DC system solver and $CEI(l)$ values obtained as described in the previous subsection. The contingencies have been ranked based on the expected value of the cascading metric and the 10 most vulnerable links have been selected. The ranking scores accounting uncertainty results slightly different compared to the deterministic case. Nevertheless, metrics drops are affected by uncertainty and some of the lines failures are more affected than others. In figure 3 are displayed CEI variabilities boxes for the 10 most vulnerable lines. It can be noticed that for the DC approximation CEI for lines l_{9-10} and l_{8-9} (rank 1 and 2) bear less uncertainty if compared to the AC case. In table 2 are displayed coefficients of variation (Cov) for the 5 most dangerous lines. Coefficient of variation is computed as ratio between standard deviation and expected value and it is a standardized measure of dispersion for the CEI distribution. The higher values confirm that AC solutions are more sensitive to the input uncertainty, which is probably due to the assumption made in order to apply the DC solver.

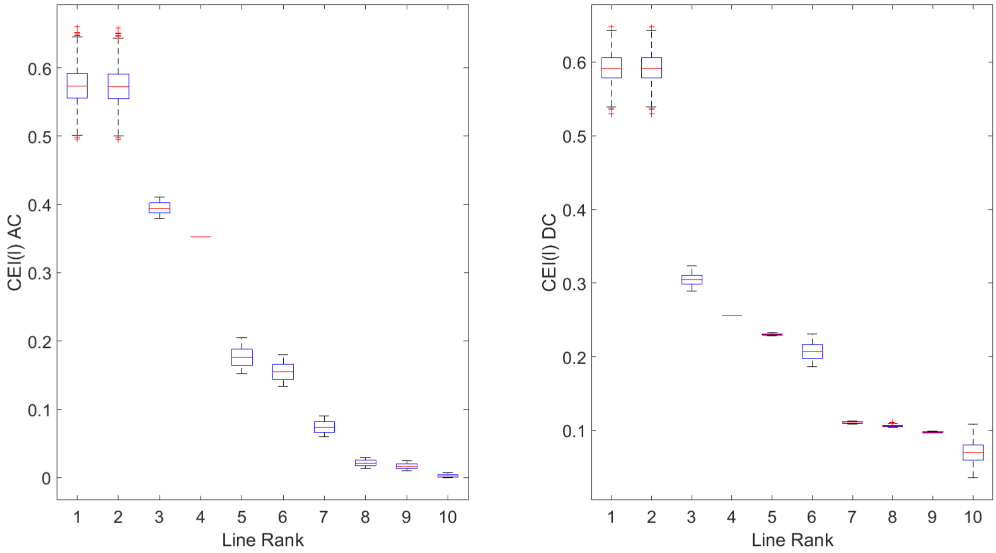

Figure 3: Variability in the CEI for the 10 most vulnerable lines.

rank	1	2	3	4	5	6	7	8	9	10
Cov_{AC}	4.5%	4.5%	2.2%	0.0%	8.0%	8.5%	11.8%	20.7%	23.6%	81.2%
Cov_{DC}	3.2%	3.2%	2.5%	0.0%	0.5%	5.4%	1.3%	1.%	0.9%	20.2%

Table 2: Variability box-plot for the ten most vulnerable lines in the IEEE 118 bus system. Coefficients of variations comparison when AC and DC power flows models are used.

Topology-based metrics and hybrid metrics results

Topology-based and extended hybrid metrics have been computed in both damaged and undamaged states. The analysis is carried as follows:

- First, adjacency matrix A and weighted adjacency matrix W are obtained for the undamaged network.
- The considered metrics $\mathcal{M}_A$ and $\mathcal{M}_W$ are computed for both A and W as described in section 4.
- The contingency analysis is performed by removing lines from the network. The matrix A and W corresponding to the graph of the damaged network are obtained and $\mathcal{M}(l)$ computed..

- Finally, vulnerabilities $\mathcal{V}(l)$ are computed as in equation 6 for each line failure. Topology-based and hybrid approach used A and W matrix respectively. The line failure are ranked based on normalized increment in the system vulnerability.

The topology-based metric which have been obtained in the approach are the graph global efficiency $\mathcal{E}_{\mathcal{G}}$, $\Lambda_{\mathcal{G}}(A)$ and $\rho_{\mathcal{G}}(A)$. These are computed using the unweighted adjacency matrix A in a purely topological way. Similarly, the extended hybrid metrics have been computed using the weighted adjacency matrix W built using susceptance matrix. These approaches account for both topology and electrical concepts. In this work $R_{\mathcal{G}}$, $\Lambda_{\mathcal{G}}(W)$ and $\rho_{\mathcal{G}}(W)$ are the hybrid metrics being analysed.

Furthermore, normalized $T_e(l)$ have been computed fore each line as in equation 12, used as an additional metric for branch ranking. Table 5 shows metric values for the undamaged IEEE 118 power network.

$\mathcal{E}_{\mathcal{G}}(A)$	$\rho_{\mathcal{G}}(W)$	$\rho_{\mathcal{G}}(A)$	$\Lambda_{\mathcal{G}}(W)$	$\Lambda_{\mathcal{G}}(A)$	$R_{\mathcal{G}}(W)$
0.216	259.56	4.112	0.3	0.0274	1565.6

Table 3: Topology-based and hybrid metrics results for the undamaged original network.

Table 5 shows the 10 most relevant links with respect to $T_e(l)$ and the variation in the vulnerability. It can be noticed that, although different vulnerability metrics produce different scores, most vulnerable lines are successfully spotted by many of the metrics. For instance, critical lines are l_{38-65}, l_{23-24}, l_{65-68}, l_{30-38} all ranked among the top 10 in 6 of the considered metrics. Relevant for the system are also lines l_{81-80} and l_{68-81} which have been identified among the ten most critical lines for 5 of the considered metrics. This result suggest that for the components ranking aims few differences can be found between hybrid and topology-based metrics.

Relative metrics drops and increments are displayed in figure 4, results have been normalized for graphical reasons. It can be noticed that some of system failures makes drop below zero some of the normalized vulnerability index (e.g. algebraic connectivity). A drop below zero means an increment in the robustness of the grid which is caused by the lines removal (e.g. line ID 146). The capability of the metrics to spot components which have unexpected negative effects for the network robustness can have an interesting features of hybrid and topology based metrics, exploitable to improve network robustness and future topology design.

Uncertainty Quantification for Topology-based and hybrid vulnerability metrics

Single loop Monte Carlo sampling procedure has been adopted as in the previous analysis and uncertain input variable propagated and effects quantified in the output. The Monte Carlo simulation number of runs and input probability distributions has been set equal to the one used for the AC and DC power flow uncertainty quantification. Results obtained for the IEEE 118 power system shows that the rankings are the same as in the deterministic case. For sake of synthesis, only results for one of the metrics are displayed, the extended betweenness.Coefficient of variation for the $T_e(l)$ have been displayed Table 5. The results shows that considered sources of uncertainty affect less these approaches, i.e. the maximum value for the Cov 0.5 $\%$ for the ten most vulnerable lines. This is a rather expected result if considered that the load demand variability do not influence any of the considered topology-based and hybrid metrics.

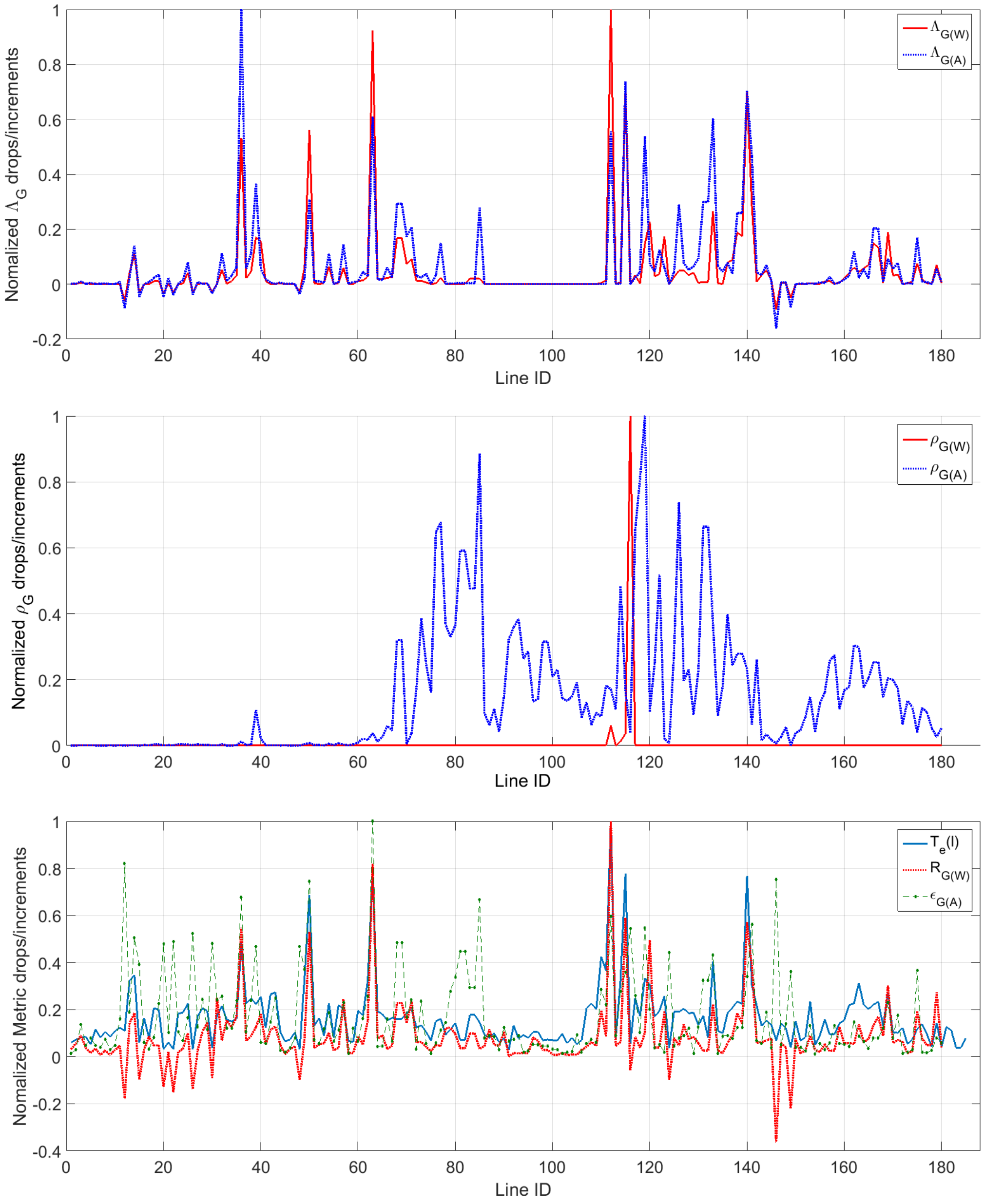

Figure 4: Comparison of relative drops and increment in different vulnerability metrics for different line contingencies.

Rank	$\mathcal{V}_{\mathcal{E}_\mathcal{G}(A)}$	$\mathcal{V}_{\rho_\mathcal{G}(W)}$	$\mathcal{V}_{\rho_\mathcal{G}(A)}$	$\mathcal{V}_{\Lambda_\mathcal{G}(W)}$	$\mathcal{V}_{\Lambda_\mathcal{G}(A)}$	$\mathcal{V}_{R_\mathcal{G}(W)}$	$T_e(l)$
1	l_{38-65}	l_{68-116}	l_{69-77}	l_{65-68}	l_{23-24}	l_{65-68}	l_{65-68}
2	l_{8-9}	l_{65-68}	l_{49-69}	l_{38-65}	l_{68-81}	l_{38-65}	l_{38-65}
3	l_{85-86}	l_{68-81}	l_{69-75}	l_{68-81}	l_{81-80}	l_{68-81}	l_{68-81}
4	l_{30-38}	l_{68-69}	l_{75-77}	l_{81-80}	l_{38-65}	l_{81-80}	l_{81-80}
5	l_{23-24}	l_{64-65}	l_{47-69}	l_{30-38}	l_{77-82}	l_{23-24}	l_{30-38}
6	l_{49-69}	l_{65-66}	l_{77-80}	l_{23-24}	l_{65-68}	l_{30-38}	l_{23-24}
7	l_{65-68}	l_{81-80}	l_{69-70}	l_{82-83}	l_{69-77}	l_{70-71}	l_{64-65}
8	l_{82-83}	l_{38-65}	l_{47-49}	l_{77-82}	l_{82-83}	l_{82-83}	l_{77-82}
9	l_{69-77}	l_{63-64}	l_{49-54}	l_{70-71}	l_{24-70}	$l_{100-103}$	l_{65-66}
10	l_{68-116}	l_{69-77}	l_{70-75}	l_{80-98}	l_{30-38}	$l_{105-108}$	l_{8-30}
rank	$\mathcal{V}_{\mathcal{E}_\mathcal{G}(A)}$	$\mathcal{V}_{\rho_\mathcal{G}(W)}$	$\mathcal{V}_{\rho_\mathcal{G}(A)}$	$\mathcal{V}_{\Lambda_\mathcal{G}(W)}$	$\mathcal{V}_{\Lambda_\mathcal{G}(A)}$	$\mathcal{V}_{R_\mathcal{G}(W)}$	$T_e(l)$
1	0.0306	0.4956	0.0196	0.3818	0.2415	0.1945	0.3423
2	0.0251	0.0299	0.0174	0.3524	0.1782	0.1593	0.2671
3	0.0230	0.0183	0.0159	0.2718	0.1698	0.1146	0.2661
4	0.0228	0.0062	0.0145	0.2662	0.1472	0.1111	0.2631
5	0.0207	0.0005	0.0133	0.2140	0.1454	0.1062	0.2349
6	0.0204	0.0004	0.0130	0.2030	0.1340	0.1026	0.1650
7	0.0183	0.0002	0.0128	0.1085	0.1300	0.0964	0.1454
8	0.0172	$4.64E-05$	0.0127	0.1016	0.1126	0.0743	0.1380
9	0.0167	$1.97E-05$	0.0116	0.0868	0.0880	0.0588	0.1256
10	0.0166	$1.86E-05$	0.0102	0.0722	0.0739	0.0529	0.1187

Table 4: Ten most vulnerable lines for the IEEE 118 system. Ranking comparison with respect to different metrics and normalized drops in the vulnerability values.

Rank	1	2	3	4	5	6	7	8	9	10
$Cov\ T_e(l)$	0.5 %	0.3%	0.5%	0.5%	0.3%	0.3%	0.4%	0.5%	0.4%	0.3%

Table 5: Comparison of coefficients of variations for the ten most vulnerable lines ranked using extended betweenness $T_e(l)$.

6 DISCUSSION AND LIMITATIONS

A modified version of the IEEE 118 nodes power network has been analysed and lines sorted with respect to their contribution to the grid vulnerability. The comparison between topology-based and hybrid approaches shows similarities in the ranking results. Some of the approaches required higher computational cost to perform the analysis, i.e. the ones based on spectral analysis of the network. The higher computational cost is required for obtain a full spectrum of eigenvalues and eigenvector for each damaged condition (and relative W, A and L). It goes without saying that the larger the network size, the higher the computational time required for the analysis, nevertheless, adjacency matrix for real world power network are often sparse matrix and therefore techniques [30] can be used to obtain just few eigenvalues. These can be used to speed up the procedure when just few eigenvalues are needed, e.g. spectral radius and algebraic connectivity.

Contingency analysis has been used to obtain a power flow-based cascading metrics, the

CEI index. Both AC and DC power flow solver have been adopted for the calculation and comparison between line ranking shows minor differences between the approaches. This is has been regarded as a confirmation of well-founded DC hypothesis for the system in exam. The comparison of the CEI index with topology-based and hybrid metrics pointed out significant differences in the ranking results. The differences in the results are possibly explained by lack of considerations about nodal power injections and withdraw of some of the approaches. The considered topology-based metrics even if enhanced in hybrid metrics cannot capture in full the operational vulnerabilities in the network. On the other hand, power-flow-based approaches included power injection and and demands magnitudes in the calculation and are hence able to spot critical components accounting changes in the operational state. Nevertheless, many of the lines ranked using CEI index resulted in a null contribution to the system vulnerability (due to null post-failure overload severity). This might be seen as a limitation of the CEI metric which has not been able to capture all the relevant aspect and information enclosed in the line failures.

Uncertainty propagated through the AC and DC methods have been quantified in the $CEI(l)$ indexes. Ranking results shows good agreement with the deterministic solution and between the different power flow solvers. The AC output seems to be more sensitive to the uncertainties in the input, which can be intuitively explained less restrictive assumptions compared to the DC method. The largest majority of the hybrid approaches make use of the DC assumptions. Generally the goodness of DC approximation should be tested and model adopted carefully[14]. Especially in scenarios where grid stress is high, such as sudden component failures or attacks, the approximation might result poor and not represent adequately the reality. Comparisons between hybrid metrics and pure topological metrics show a good agreement in the line ranking although some of them, i.e. ranking based on drops in spectral radius, differs substantially. This might be due to limitation of the latter metric or computational inaccuracies.

7 CONCLUSIONS

The future electric power grid is a complex network which have to deal with uncertainty from different sources. The correct functioning of the system and components will strongly depend on the operational context. Therefore provide easy to follow guidances and robustness metrics is uttermost important point. The metrics have to be capable of capturing uncertainties and variability in the network dynamic and as well intrinsic topological weaknesses in a reliable way. In the presented work different vulnerability metrics have been compared. The metric to be used in the analysis have o be carefully selected accordingly to its aims and without forgetting underling assumptions or underestimating on the uncertainty affecting the problem. The metrics ability to spot system criticality and in ranking important components has been discussed.Link removal and uncertainty effects have been analysed and relative drops or increments in the metrics were computed. The IEEE 118 power grid has been used as reference case study. The AC and DC power flow cascading metrics have been compared against topology-based and hybrid metrics often used in power grid vulnerability studies. The power grid robustness against cascading and vulnerable lines have been identified using different approaches and uncertainty quantified in the output and models.

REFERENCES

[1] R. Rocchetta, Y.F. Li, E. Zio, *'Risk assessment and risk-cost optimization of distributed power generation systems considering extreme weather conditions'*. Reliability Engineer-

ing & System Safety, Volume 136, 4 -61, 2015.

[2] G. A. Pagani, M. Aiello, *'From the grid to the smart grid, topologically'*. Physica A: Statistical Mechanics and its Applications, 2015.

[3] E. Zio and T. Aven, *'Uncertainties in smart grids behavior and modeling: What are the risks and vulnerabilities? How to analyze them?'*. Energy Policy Volume 39, 6308-6320, 2011.

[4] A. Kott, T. Adbelzaher, *Resiliency and Robustness of Complex Systems and Networks*. Adaptive Dynamic Resilient Systems,19, 1387-1401, 2004.

[5] Cuadra, Lucas, Salcedo-Sanz, Sancho, Del Ser, Javier, Jimnez-Fernndez, Silvia, Geem, Zong Woo, *A Critical Review of Robustness in Power Grids Using Complex Networks Concepts*.Energies Volume 8, 9211-9265, 2015.

[6] Rosas-Casals M.; S. Bologna; E.F. Bompard; G. D'Agostino; W. Ellens; G. A. Pagani; A. Scala; T. Verma, *'Knowing power grids and understanding complexity science'*. Int. J. of Critical Infrastructures,Volume 11, 4-14, 2015.

[7] E.F. Bompard, R. Napoli, F. Xue, *'Analysis of structural vulnerabilities in power transmission grids'*. International Journal of Critical Infrastructure Protection, Volume 2, 5 - 12, 2009.

[8] E. Bompard, D. Wu, F. Xue, *'Structural vulnerability of power systems: A topological approach'*. Electric Power Systems Research, Volume 81, 1334-1340, 2011.

[9] Y. Koç, M. Warnier, P. Van Mieghem, R. E. Kooij, F. M.T. Brazier, *'The impact of the topology on cascading failures in a power grid model'*. Physica A: Statistical Mechanics and its Applications, Volume 402, 169-179, 2014.

[10] F. Xiao, McCalley, J.D. C., *'Power System Risk Assessment and Control in a Multiobjective Framework'*. Power Systems, IEEE Transactions on Volume 24, 78-85, 2009.

[11] Min Ouyang, Zhezhe Pan, Liu Hong, Lijing Zhao, *'Correlation analysis of different vulnerability metrics on power grids'*. Physica A: Statistical Mechanics and its Applications, Volume 396, 204 - 211, 2014.

[12] P. Van Mieghen, *'Graph Spectra For Complex Networks'*. Cambridge University Press. 2011.

[13] . Koç, M. Warnier, P. Van Mieghem, R. E. Kooij, F. M.T. Brazier, *'A topological investigation of phase transitions of cascading failures in power grids'*. Physica A: Statistical Mechanics and its Applications Volume 415, 273-284,2014.

[14] Van Hertem, D., Verboomen, J., Purchala, K., Belmans, R., Kling, W.L.*'Usefulness of DC power flow for active power flow analysis with flow controlling devices'*. AC and DC Power Transmission, 58-62, 2006. ACDC 2006.

[15] R. Mena, M. Hennebel, Y.F. Li, C. Ruiz, E. Zio, *'A risk-based simulation and multi-objective optimization framework for the integration of distributed renewable generation and storage'*. Renewable and Sustainable Energy Reviews, Volume 37, 778-793, 2014.

[16] Dwivedi A., Xinghuo Y., Sokolowski P., *'Identifying vulnerable lines in a power network using complex network theory'*. Industrial Electronics, 2009. ISIE 2009. IEEE International Symposium on, 18-23, 2009.

[17] K.S. Turitsyn, P.A. Kaplunovich, *'Fast Algorithm for N-2 Contingency Problem'*. System Sciences (HICSS), 2013 46th Hawaii International Conference on.

[18] R. Rocchetta, M. Broggi, E. Patelli, *'Efficient Epistemic-Aleatory Uncertainty Quantification: Application to the NAFEMS challenge problem'*. NAFEMS World Congress 2015, At San Diego, CA, 2015

[19] Jamakovic A., Uhlig S., *'On the relationship between the algebraic connectivity and graph's robustness to node and link failures'*. Next Generation Internet Networks, 3rd EuroNGI Conference on, 96-102, 2007.

[20] E.R. van Dam, R.E. Kooij, *'The minimal spectral radius of graphs with a given diameter'*. Linear Algebra and its Applications, Volume 423, 2-3, 2007.

[21] J. McCalley, M. Ni, V. Vittal, T. Tayyib, *'Online risk-based security assessment'*. IEEE Transactions on Power Systems Volume 18, 258-265, 2003.

[22] P. Henneaux, *'Probability of failure of overloaded lines in cascading failures'*. International Journal of Electrical Power & Energy Systems, Volume 73, 141-148, 2015.

[23] Greene S., Dobson I., Alvarado F.L.,*'Contingency ranking for voltage collapse via sensitivities from a single nose curve'*. Power Systems, IEEE Transactions on, Volume 14, 232-240, 1999.

[24] R. D. Zimmerman, C. E. Murillo-Snchez,, R. J. Thomas, *MATPOWER Steady-State Operations, Planning and Analysis Tools for Power Systems Research and Education*, Power Systems, IEEE Transactions on, Volume 26, no. 1, 12-19, Feb. 2011

[25] Guan-sheng Peng, Jun Wu, *Optimal network topology for structural robustness based on natural connectivity*, Physica A, Volume 443, 212220, 2016.

[26] S.Zhang, I. Dobson, F.L. Alvarado, *'Quantifying transmission reliability margin'*. Electrical Power and Energy Systems 26, 697702, 2004.

[27] M. Shahidehpour, Y.Wang, *'Communication and Control in Electric Power Systems'*. IEEE Press Power Engineering Series, 477-48, 2003.

[28] Monfared, M. A. S., Jalili, M., Alipour, Z.*'Topology and vulnerability of the Iranian power grid'*. Physica A: Statistical Mechanics and its Applications, Volume 406, 24 - 33, 2014.

[29] Chen, Y.C., Dominguez-Garcia, A.D., Sauer, P.W., *'Generalized injection shift factors and application to estimation of power flow transients'*. North American Power Symposium (NAPS), 1-5, 2014.

[30] Lehoucq R.B., D.C. Sorensen, *'Deflation Techniques for an Implicitly Re-Started Arnoldi Iteration'*. SIAM J. Matrix Analysis and Applications, Volume 17, 789821, 1996.