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 SERE 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 very reliable systems, nevertheless outages and electricity shortfalls are common events and have the potential to produce significant social and economic consequences. It is important to reduce the likelihood of those severe accidents by assuring safe operations and robust topologies. The grid safety relies on accurate vulnerability measures, control schemes and good quality information. For instance, in 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). An exhaustive failure list is often not treatable, therefore a selection or ranking is performed to help in the choice. In order to better understand the power network weakness and strengths a variety of robustness metrics have been introduced in literature, although many do not account or partially account for uncertainties which might affect the analysis. In this work power network vulnerability to failure events is analysed and single line outages (N-1 contingencies) have been ranked using different metrics (i.e. topology-based, flow-based and hybrid metrics). Sources of uncertainty such as power demand variability and lack of precise knowledge on the network parameters have been accounted for and its effect on the component ranking quantified. A modified version of the IEEE 118 bus power network has been selected as representative case study. The assumption underpinning the methodologies and the vulnerability results also accounting uncertainty are discussed.*

1 INTRODUCTION

Robustness of power grids is defined as the degree to witch the network is able to withstand an unexpected event without degradation in performance [1]. A closely related concept is the vulnerability, which is sometime regarded as lack of robustness. Robustness and vulnerability are nowadays major concerns for the future power networks. Historically, power networks were developed to distribute electricity 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. 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 this traditional design has deeply changed, the allocation of renewable energy sources are making its behaviour less predictable and vulnerability assessments less reliable, mainly due to the considerable amount of uncertainty injected in the system [2]. Non-radial meshed topologies and not classical structures are likely to became more common in the future [3]. The presented scenario highlights the need of develop more reliable and robust frameworks for power grid vulnerability analysis (i.e. adopting sophisticated uncertainty quantification techniques), as well as the need of define enhanced metric for the assessment and identification of operational and structural risks. In order to improve robustness it is important to understand the role played by the variability the grid state variables (e.g. power produced, loads, voltage phases, magnitudes.) and by the imprecisely known network parameters (flow and voltage limits, topology, line resistances, etc.). Structural weaknesses have to be identified to design better topologies (e.g. by efficient ranking of components failures) and mitigate likelihood of unexpected hazardous situations .

In literature, a wide range of indexes have been proposed for vulnerability and robustness assessment, e.g. using realistic simulation of network response and power-flow solution (“power-flow-based metrics”) or based on topological analysis of networks, using techniques founded on complex network theory [4]. The latter are computed using pure topological approaches (i.e. ‘topology-based metrics’) or enhanced by including electrical engineering concepts in the analysis (i.e. ‘hybrid metrics’). 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 ($\mathcal{B}_e$) M. Ouyang et al. [6] analysed correlation of six topology-based vulnerability metrics respect to multiple components failure. E. Bompard et al. [5] compared two hybrid metrics (i.e. extended betweenness and net-ability) in their ability to rank components failures. Power-flow-based metric, such as system cascading index (CEI), has been applied to estimate likelihood and extent of cascading failures [7].

To the Authors knowledge, few among the reviewed works quantified the effect of uncertainty in the metrics and compared the different ranks of component failures. Hence, further comparison between different indices, with particular regard to the uncertainties affecting the different approaches seems to be needed. In this survey vulnerability metrics are compared, with particular regard to the line failures ranking. Power demand uncertainty and system parameters (line power flow limits) uncertainty are analysed and their effect quantified. 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 in ranking critical components and spot network weaknesses, also accounting uncertainty.

The paper is structured as follows:
Power network modelling is introduced in Section 2. Contingency analysis and uncertainty modelling are described in in Section 3. In Section 4 robustness and vulnerability concepts are discussed and the metrics defined. A case study is defined in Section 5 and results displayed. Limitation faced and further discussions are presented in Section 6. 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 rewritten 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 can be used analyse spectral graph proprieties of networks such as its eigenvalues eigenvectors. Spectral proprieties of graph $\mathcal{G}$ bears valuable information about the network the graph represent and some eigenvalues can be associated to its robustness [8]. Further details are going to be discussed in Section 4.
The Laplacian L_A of the adjacency matrix A is defined as [9]:

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

where A is the adjacency matrix and D_A is the diagonal matrix of degrees for A. The matrix Laplacian can be computed using the weighed adjacency matrix W (i.e. including electrical concepts such as susceptances).

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. 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 [10]:

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

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

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, neglecting power loses and reactive power management. It has been widely used to alleviate the computational cost of numerically intensive codes and it has always a feasible solution. The majority of works which aimed at including electrical engineering concepts in graph theoretical approaches made use of the DC assumption, e.g. in defining weighted adjacency matrix of the graph. The DC power flow formulation can be written as follows [10]:

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

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

- Flat voltage profile $|V_i| = 1$ per unit. $\forall\ i \in \mathcal{N}$
- 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 [10]. 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 [4].

3 TREATMENT OF UNCERTAINTY

Generally speaking, uncertainty can be separated in two groups, the so called aleatory and epistemic uncertainties [11]. 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 well-recognized sources of uncertainty are electricity price volatility, load power demand and environmental variability, model assumption (e.g. DC or AC power flow, contingency selection). The sources of uncertainty investigated in this work are:

- Uncertainty in the line emergency rating (line power flow constrain) 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 [12]. 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 i ($P_{L,i}$) can be described by a Normal distribution [13].The parameter of the distribution can be estimated from historical records of load demand per node.

A 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 for further vulnerability assessment and contingency ranking. The algorithm allows obtaining a probabilistic description of the outputs variability, i.e. the output probability distribution functions with respect to the input uncertainties and wider prospective on the result of the ranking.

A contingency in power networks is defined as the unexpected failure of one of its components (e.g. links, nodes, generators, transformers) [13]. 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. In power grid reliability and risk assessment, common practice consists in selecting a subset of the more threatening contingencies based on expert opinion or by some identification procedure [15]. In this work, the $N-1$ single line trips are analysed and the most threatening failures ranked using different metrics.

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 [6]. 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 [4]:

$$\mathcal{V}(C_i) = \frac{\mathcal{M} - \mathcal{M}(C_i)}{\mathcal{M}} \tag{5}$$

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 simulating the outages by both AC power flow contingency analysis and its linear DC approximation. Generally speaking, a "cascading" is a sequential successions of dependent events [18].The metric adopted to assess the cascading overload vulnerability is defined as follows [18]:

$$CEI(C_i) = \sum_{l \in \mathcal{L}} \mathcal{P}(C_l|C_i) SevOL_l(C_i) \tag{6}$$

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 [13]. The continuous severity function for overload is specifically defined for each link l (distribution lines and transformers) and it measures the extent of violation in terms of excessive power flow ratio PR_l. PR_l is the ratio between active power flowing in the line P_l and its emergency rating $P_{emerg,l}$. The expression for the continuous severity due to overload $(SevOL_l)$ of a line l is findable in [13].

$$SevOL_l = d * PR_l + c \quad for \quad PR_l \geq PR_l^{min} \tag{7}$$

where $SevOL_l$ is zero for values of the flow rating less than a safety limit PR_l^{min}=0.9. The deterministic limit for the violation of line l is PR_l=1, the near violation region is 0.9≤ PR_l <1, and the value PR_l under 0.9 is regarded as safe, d=10 and c=-9.

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 near violation scenarios have not null risk. The probability of cascading trip of line k after an initiating contingency i can be expressed as in [7]:

$$\mathcal{P}(C_j|C_i) = \frac{P_j(C_i,\zeta) - P_{0,j}(\zeta)}{P_{trip,j}(C_i,\zeta) - P_{0,j}(\zeta)} \tag{8}$$

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 8 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 for $P_j(C_i,\zeta) \geq 0.9P_{emerg,j}$.

Topology-based and hybrid metrics

Power network vulnerability can by pure topological analysis of the grid structure. These approach use unweighted adjacency matrix A, components are regarded as identical and no rough electrical concept is included in the analysis [4]. Similarly, hybrid metrics adopt complex network concepts 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 $B_{i,k}$. The analysed metrics in this paper are: graph spectral radius, algebraic connectivity, effective graph resistance, graph global efficiency [22] and extended betweenness [5].

In spectral analysis of graphs, the largest eigenvalue of the adjacency matrix is known as graph spectral radius ($\rho_\mathcal{G}$). Few works attempted to relate spectral radius to the power grid vulnerability and relatively small values have been considered as indicator of robustness [8]. Another important metrics obtained 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 metric $\Lambda_\mathcal{G}$ is used as indicator of the level of connection between nodes in a graph,and is regarded as a basic indication of the network robustness level [16]. The effective graph resistance ($R_\mathcal{G}$) is an hybrid metric which have been sometimes related to the power grid vulnerability [8]. 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 $j.R_\mathcal{G}$ can be obtained as follows:

$$R_\mathcal{G} = \sum_{i=1}^{N-1} \frac{1}{\mu_i} \tag{9}$$

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 ($\mathcal{E}_G$) and betweenness. The efficiency of a network is defined as the average of inverses of the distance for all nodes. For calculation of $\mathcal{E}_G$ the reader is reminded to [22]. Betweenness has been recently used in [14] to identify most vulnerable lines in power systems. The extended betweenness ($T_e(l)$) has been introduced in [5] 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:

$$T_e(l) = max(|\sum_{g \in G}\sum_{d \in Ld} C_g^d f_l^{gd}|)\ l \in \mathcal{L} \tag{10}$$

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 described in [5].

5 CASE STUDY

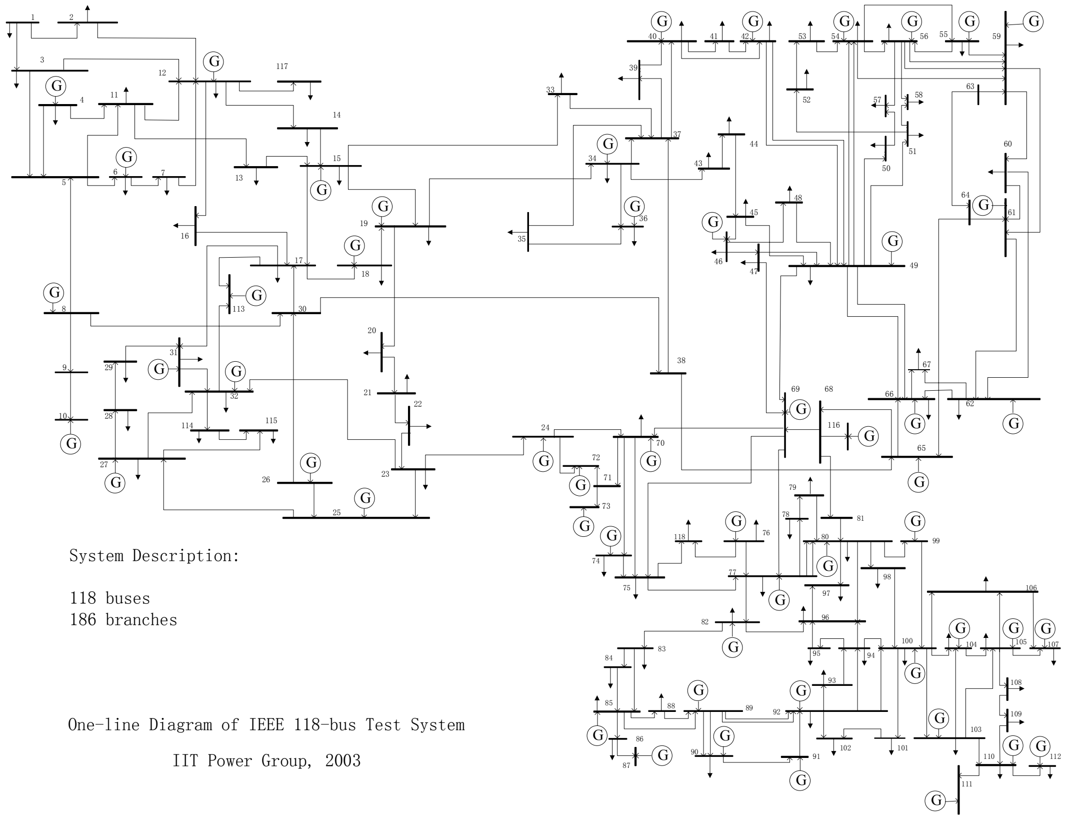

Figure 1: The IEEE 118 bus test system [21].

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 load demand and lines emergency ratings data are available in [20]-[21]. Figure 1 displays the network structure and generators location. The original network data have been modified in order to simulate a condition of higher stress for the network. Increment in the load demand of 30 $\%$ and $P_{emerg,l}$ for all the lines l in the links set $\mathcal{L}$ 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 indices CEI computed and line outages ranked. The analysis is performed as follows:

- First, AC or DC approach is used to compute the optimal power production subject to line flow limits, generation constraints and load demanded.
- The contingency analysis is performed by removing one line at a time from the system. The AC or DC methods simulate the power flows redistribution in the branches given the optimal power scheduled.
- Finally, the $CEI(l)$ are computed for each contingency based on the equation 6. Line vulnerability are ranked and ordered based on the CEI values.

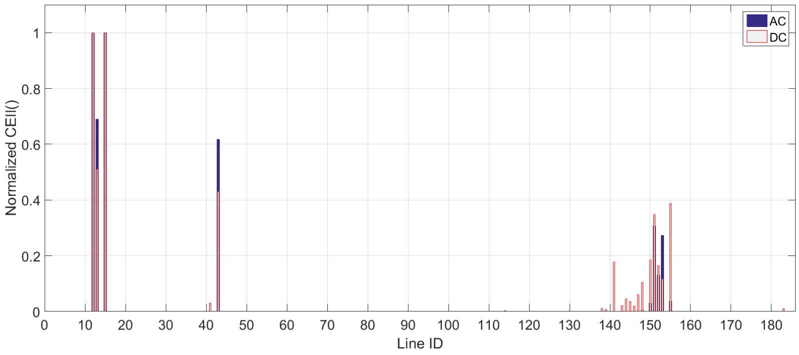

Figure 2: Normalized CEI results comparison between AC solution and and its DC approximation. On the X-axis the failed line (Line ID).

Figures 2 shows the optimal power production computed by means of the AC and DC method, respectively. The Y-axis shows the normalized CEI results and the X-axis the line identification number (ID). It can be noticed that DC power flow, when compared to AC power flow, overestimate the cascading indices for some of the contingency listed (e.g. lines ID 141-150) and underestimate them for others e.g line ID 13, 43, 153 (l_{8-5}, l_{26-30}, l_{89-92}). This is mainly due to the approximate percentage of rating PR_k obtained in the DC approach. Nevertheless, the 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. Results are summarized in Table 5 which displays the 10 most vulnerable lines in the system, with respect to all the metrics analysed. In both AC and DC flow-based approaches the ranking results are fairly similar and similar to previous studies, see as example [19]. The most threatening lines result to be l_{9-10}, l_{8-9}, l_{8-5}, l_{26-30} for both cases.

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, but with different aims, 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. The CEI variabilities boxes for the 10 most vulnerable lines are shown in figure 3. 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 1 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.

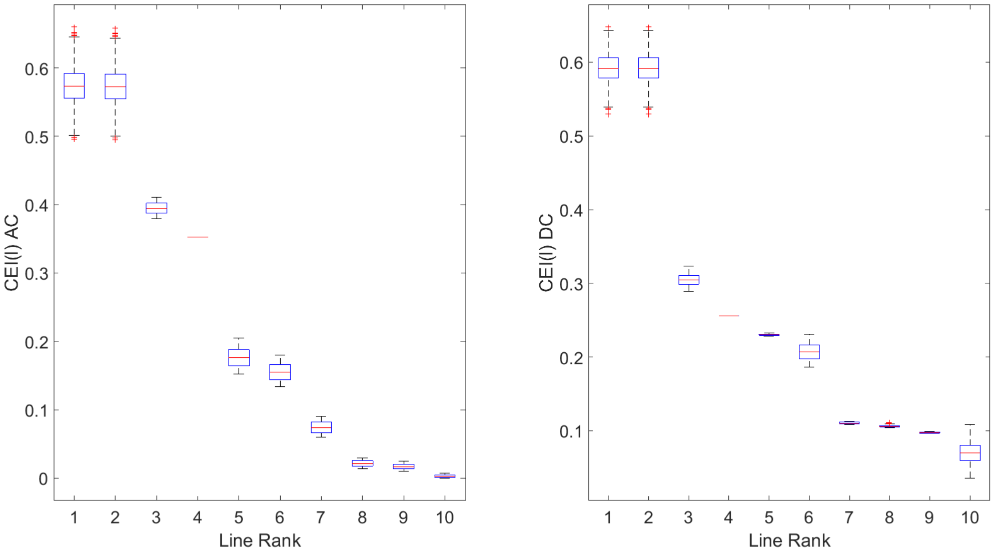

Figure 3: Variability in the normalized cascading index CEI for the 10 most vulnerable lines. Comparision between AC and DC power flow solutions.

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 1: 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 adjacency matrix A and W respectively, 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 5 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 10, 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 2: 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. Although different vulnerability metrics produce different scores, the most vulnerable lines are successfully spotted. 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. Similarly, lines l_{81-80} and l_{68-81} have been identified as critical by 5 metrics. This result suggest that for the components ranking purposes few differences can be found between hybrid and topology-based metrics.

Relative metrics drops and increments are displayed in figure 4, the results have been normalized for graphical reasons. It can be noticed that some of the lines failure cause a drop below

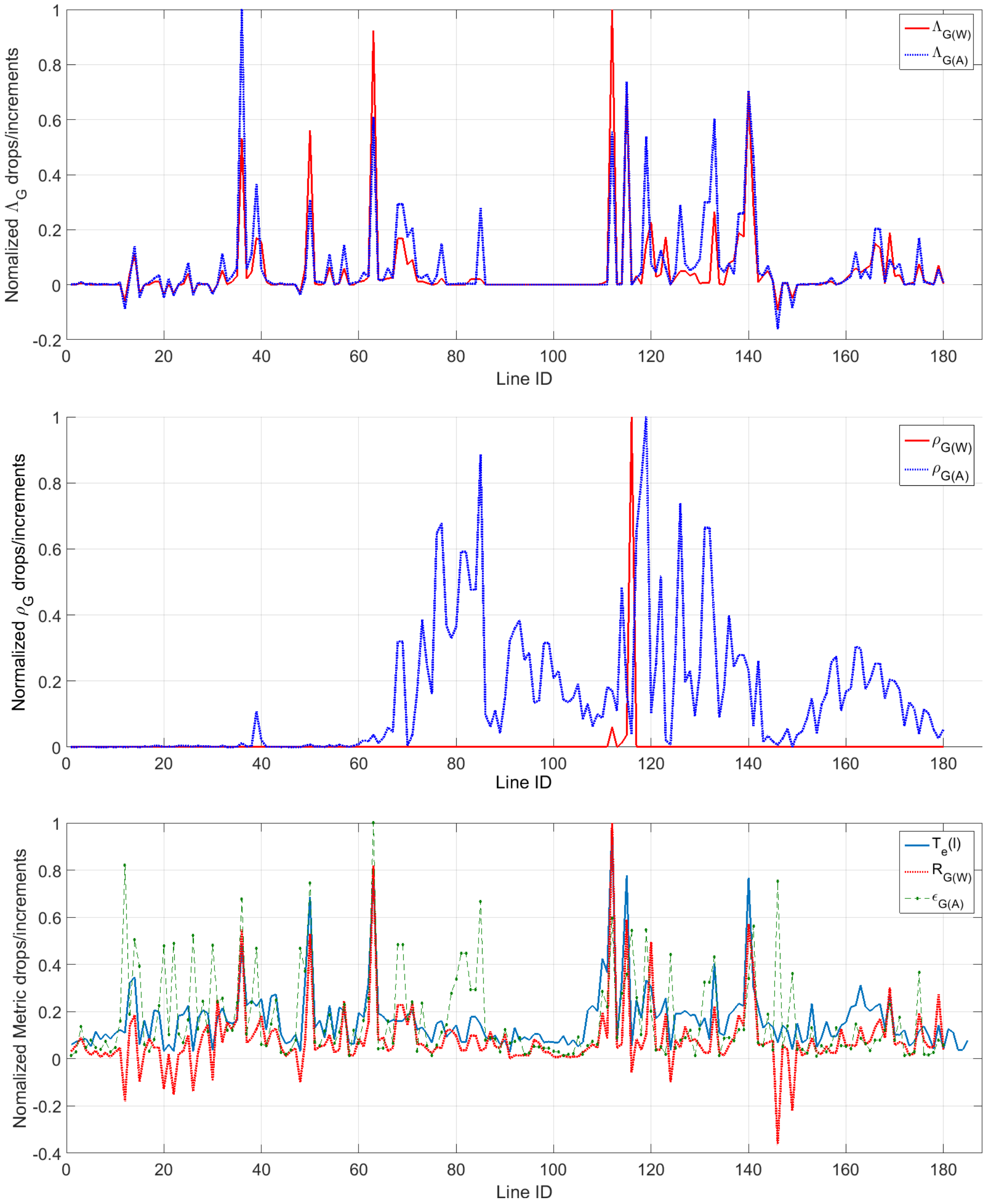

Figure 4: Comparison of relative drops and increment in vulnerability metrics, Y-axis, due to single line failures(X-axis).

Rank	$\mathcal{V}_{\mathcal{E}_\mathcal{G}(A)}$	$\mathcal{V}_{\rho_\mathcal{G}(W)}$	$\mathcal{V}_{\rho_\mathcal{G}(A)}$	$\mathcal{V}_{\Lambda_\mathcal{G}(W)}$	$\mathcal{V}_{\Lambda_\mathcal{G}(A)}$	$\mathcal{V}_{R_\mathcal{G}(W)}$	$T_e(l)$	CEI_{AC}	CEI_{DC}
1	l_{38-65}	l_{68-116}	l_{69-77}	l_{65-68}	l_{23-24}	l_{65-68}	l_{65-68}	l_{9-10}	l_{8-9}
2	l_{8-9}	l_{65-68}	l_{49-69}	l_{38-65}	l_{68-81}	l_{38-65}	l_{38-65}	l_{8-9}	l_{9-10}
3	l_{85-86}	l_{68-81}	l_{69-75}	l_{68-81}	l_{81-80}	l_{68-81}	l_{68-81}	l_{8-5}	l_{8-5}
4	l_{30-38}	l_{68-69}	l_{75-77}	l_{81-80}	l_{38-65}	l_{81-80}	l_{81-80}	l_{26-30}	l_{26-30}
5	l_{23-24}	l_{64-65}	l_{47-69}	l_{30-38}	l_{77-82}	l_{23-24}	l_{30-38}	l_{89-90}	l_{91-92}
6	l_{49-69}	l_{65-66}	l_{77-80}	l_{23-24}	l_{65-68}	l_{30-38}	l_{23-24}	l_{89-92}	l_{89-90}
7	l_{65-68}	l_{81-80}	l_{69-70}	l_{82-83}	l_{69-77}	l_{70-71}	l_{64-65}	l_{89-91}	l_{88-89}
8	l_{82-83}	l_{38-65}	l_{47-49}	l_{77-82}	l_{82-83}	l_{82-83}	l_{77-82}	l_{91-92}	l_{82-83}
9	l_{69-77}	l_{63-64}	l_{49-54}	l_{70-71}	l_{24-70}	$l_{100-103}$	l_{65-66}	l_{88-89}	l_{89-91}
10	l_{68-116}	l_{69-77}	l_{70-75}	l_{80-98}	l_{30-38}	$l_{105-108}$	l_{8-30}	l_{85-89}	l_{89-92}
Rank	$\mathcal{V}_{\mathcal{E}_\mathcal{G}(A)}$	$\mathcal{V}_{\rho_\mathcal{G}(W)}$	$\mathcal{V}_{\rho_\mathcal{G}(A)}$	$\mathcal{V}_{\Lambda_\mathcal{G}(W)}$	$\mathcal{V}_{\Lambda_\mathcal{G}(A)}$	$\mathcal{V}_{R_\mathcal{G}(W)}$	$T_e(l)$	CEI_{AC}	CEI_{DC}
1	0.031	0.4956	0.020	0.382	0.241	0.194	0.342	0.5931	0.57365
2	0.025	0.0299	0.017	0.352	0.178	0.159	0.267	0.5931	0.57246
3	0.023	0.0183	0.016	0.272	0.170	0.115	0.266	0.3028	0.39562
4	0.023	0.0062	0.014	0.266	0.147	0.111	0.263	0.2549	0.35366
5	0.021	0.0005	0.013	0.214	0.145	0.106	0.235	0.2297	0.17620
6	0.020	0.0004	0.013	0.203	0.134	0.103	0.165	0.2066	0.15594
7	0.018	0.0002	0.013	0.109	0.130	0.096	0.145	0.1099	0.07426
8	0.017	0.0000	0.013	0.102	0.113	0.074	0.138	0.1056	0.02133
9	0.017	0.0000	0.012	0.087	0.088	0.059	0.126	0.0973	0.01678
10	0.017	0.0000	0.010	0.072	0.074	0.053	0.119	0.0691	0.00246

Table 3: Ten most vulnerable lines for the IEEE 118 system. Ranking comparison with respect to different metrics and normalized drops in the vulnerability.

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 approach and input distributions used are the same as for the AC and DC power flow uncertainty quantification. The 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 in Table 4.

The results shows that considered sources of uncertainty affect less these approaches, i.e. the

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

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.

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. Spectral analysis of the network require higher computational cost for obtaining a full spectrum of eigenvalues and eigenvector for each damaged condition (and relative W, A and L).

Contingency analysis has been used to obtain a power flow-based cascading metrics, the CEI indices. Both AC and DC power flow solver have been adopted for the calculation and comparison between line ranking showing minor differences between the approaches. This has been regarded as a confirmation of well-founded DC hypothesis for the system in exam. The comparison of the CEI indices with topology-based and hybrid metrics suggest significant differences in the ranking. The differences can be 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 demands magnitudes in the calculation and hence able to identify 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 show 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 due to the 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[10]. 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 providing 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 this paper different vulnerability metrics have been compared in their ability to spot system criticality and ranking important components.The effects of uncertainty have been analysed and relative drops or increments in the metrics discuses and compared to the same approaches with no uncertainty accounted for. The IEEE 118 power grid has been used as case study. The AC and DC power flow cascading metrics showed higher uncertainty in the outputs if compared to topology based metrics. This is due to operational variability not fully accounted in the latter approaches and to the different assumptions. In conclusion, the selection of metrics for vulnerability assessment of power grids have o be selected carefully. The analyst should account both influence of the underling model assumptions and system variability. Wrong consideration of uncertainty can lead to imprecise considerations on the system vulnerability and in the worst case to misleading results on its robustness and reliability.

REFERENCES

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

[2] 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.

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

[4] 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.

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

[6] 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.

[7] 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.

[8] . 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.

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

[10] 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.

[11] 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

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

[13] R. Rocchetta, Y.F. Li, E. Zio, *'Risk assessment and risk-cost optimization of distributed power generation systems considering extreme weather conditions'*. Reliability Engineering & System Safety, Volume 136, 4 -61, 2015.

[14] 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.

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

[16] 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.

[17] 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.

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

[19] 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.

[20] 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

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

[22] 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.