Reliability Engineering and System Safety 217 (2022) 108085

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Identifying and assessing power system vulnerabilities to transmission asset outages via cascading failure analysis

Blazhe Gjorgiev, Giovanni Sansavini [*]

Reliability and Risk Engineering Laboratory, Institute of Energy and Process Engineering, Department of Mechanical and Process Engineering, ETH Zurich, Switzerland

ARTICLE INFO

Keywords:
Power system
Vulnerability
Cascading failures
Power flow
Optimization

ABSTRACT

Power systems as critical infrastructure are an integral part of human society and are therefore of paramount importance to modern life. Vulnerabilities in the system, that are revealed either by accidental or deliberate events, can cause large losses of power supply with sever social and economic consequences. A tool that identifies the vulnerabilities in a power system can provide the operators the means to support reliable power system operations. This paper presents a methodology for power system vulnerability assessment that couples an AC based cascading failure simulation model and a meta-heuristic optimization procedure. The objectives of the assessment are to (1) rank the most important branches in the transmission grid, and (2) identify sets of branches if simultaneously tripped will cause the cascade with highest intensity. The first objective is achieved by ranking the criticality of the branches using two criteria (i) the impact that each branch failure has on the DNS and (ii) the frequency of line overload. The second objective is achieved by hard linking an AC based cascading failure simulation model and a meta-heuristic based optimization procedure. The methodology allows the generation and the identification of vulnerability scenarios, and therefore, provides insights that can be used by operators in developing strategies to minimize the effects of accidental and deliberate events. The algorithm developed for the purpose of this study is applied to the IEEE 118-bus test system and the Swiss power grid. The results demonstrate the capability of the proposed methodology for assessing power system vulnerability.

1. Introduction

Power systems as a critical infrastructure are an integral part of human society and are therefore of paramount importance to modern life. They are one of the most complex engineered systems ever build, aiming to provide a reliable power supply [1]. Power systems vulnerabilities are reviled either by accidental or deliberate events [2]. As accidental events are considered the random failures and natural hazards [3], and as deliberate events are considered the physical attacks, cyber-attacks, and electromagnetic pulses (EMP) [4]. An extensive body of research on power system vulnerability, performed in the past decades, highlights the relevance of the topic [3]. The vulnerability of a system can be defined as the “manifestation of the inherent states of the system that can be exploited by an adversary to harm or damage the system” [5].

Scientific literature reviles variety of models and methods used for power system vulnerability analysis. In general, they can be placed in two categories: (1) topological approaches; and (2) flow-based approaches. The topological approaches are based on network connectivity and the complex network concept [6, 7]. They rely only on information on the gird topology, and are computationally efficient [8]. The flow-based approaches are based on the power flow dynamics and physical characteristics of the power grid. They rely on the information of the physical characteristics of the grid, and can be computationally expensive [9]. A more detailed review of all types of methods used in power system vulnerability analysis is present in [3].

A topological model for the identification of groups of most critical elements in the Italian high-voltage grid is presented in [8]. The model identifies the important groups by applying the betweenness centrality of groups of nodes and groups of edges, and the variation in network connection efficiency. An integrated topological and reliability framework, comprising different centrality measures, for assessing the vulnerability of the high-voltage Iranian power grid is introduced in [10]. The paper shows that the reliability characteristics differ from the topological results, because they are mostly uncorrelated. Eusgeld et al. [11] use topological analysis to identify the most relevant parts for system vulnerability, supplemented by a physical analysis to understand better the mechanisms responsible for these vulnerabilities. Similarly,

[*] Corresponding author.
E-mail address: sansavig@ethz.ch (G. Sansavini).

https://doi.org/10.1016/j.ress.2021.108085
Received 1 July 2021; Received in revised form 6 September 2021; Accepted 21 September 2021
Available online 25 September 2021

[12] presents an extended topological approach that, besides the regular topological metrics, considers the line flow limits and applies a real power-flow allocation over lines. Furthermore, topological models are used in combination with probabilistic safety assessment (PSA), where fault trees are applied to identify and rank critical components in the power grid [13]. A statistical model for estimating the probability of restoring power to the electric grid before a determined time after a blackout is presented in [14]. This developed knowledge can be used to inform event tree calculations in PSA models. In general, the topological approaches are criticized for their inability to capture the physical process occurring in the power grids, despite the attempts to perform additional physical analysis.

On the other hand, the main arguments against the flow-based approaches are their complexity and computational inefficiency. However, these approaches are widely used today, e.g. a DC power flow based method that exploits game theory is used to assess the vulnerability of a power system [15]. Similarly, [16] introduces an optimization method in a game theory framework, which utilizes linear approximation AC power flow and aims to identify critical components in a power system. The DC power flow based OPA model [17] and the AC power flow based Manchester model [18] are the most recognized cascading failure analyses models. In [19], the criticality of individual components of power systems is assessed via AC based cascading failure model considering multi-element failures. The proposed approach builds upon the Fussell-Vesely importance measure quantifying the performance decrease ratios due to the loss of grid elements. A flow-based approach that utilizes a novel mixed integer linear programming optimization framework is described in [20]. The study assesses the impact of several natural hazards on the grid infrastructure employing failure and recovery probabilities for system components. Similarly, [21] proposes a resilience enhancement framework for interdependent gas and power grids. The framework utilizes a multi-objective genetic algorithm to find the optimal resilience enhancement strategies. A study of the vulnerability and reliability of a power system with various levels of penetration of renewables is performed in [22]. The results show that the vulnerability and reliability are affected by the renewable sources and the electrical interconnections. Abedi et al. [23] compare a DC and AC approaches for vulnerability, reliability, and contingency assessment of a power grid. The results show that the DC model significantly underestimates the reliability, and, therefore, conclude that the AC models should be prioritized.

A comparison of the criticality of power grid complements is performed using multiple cascading failure models in [24]. Different models show some inconsistencies when allocating grid assets criticality, which indicates that cascading failure analysis is still an active field of research. Cascading failure models are known for being capable of performing comprehensive cascading failure analysis and assessing the vulnerability of the power grids. However, their identification of the critical components mainly focuses on the impact on the demand not served (DNS) caused by a single branch failure or by sets of randomly generated contingencies. The methodology proposed in [25] goes further, combining a DC based cascading failure model and a stochastic “Random Chemistry” (RC) algorithm, to identify large collections of multiple contingencies that initiate large cascading failures. Yet, this approach does not utilize optimization to determine the sets of contingencies causing the worst blackouts (i.e. DNS). Furthermore, methods using optimization are also applied to uncover small subsets of events with high impact [26, 27]. However, these methods rely primarily on detecting limit violations and load shedding actions, and they do not simulate the full propagation of disturbance events, i.e. do not perform cascading failure analyses.

We address this research gap by introducing a vulnerability assessment methodology that couples an AC based cascading failure simulation model and a meta-heuristic optimization procedure. The use of cascading failure analyses is motivated by the fact that modern power systems, despite the multiple layers of protective schemes, are still experiencing blackouts that are mainly caused by cascading failures [28, 29]. The objectives of the proposed methodology are to: (1) provide ranking of the most important branches in the transmission grid, and (2) identify sets of branches that will cause the cascade with the highest intensity if simultaneously tripped. The first objective is achieved by ranking the criticality of the branches using two criteria (i) the impact that each branch failure has on the DNS and (ii) the frequency of line overload. The second objective is achieved by hard linking an AC based cascading failure simulation model and a meta-heurist based optimization procedure. This link allows for optimal identification of vulnerabilities that have the potential to spread within the power grid, while considering automatic and manual system responses. The algorithm developed for the purpose of this study is applied to the IEEE 118-bus test system and the Swiss power grid. The results provide a ranking of the branches according to the two different criteria and identify the sets of branches that are most critical to system security. The potential application of these results includes asset upgrade and guidance for operators on implementation of procedures for improving the system response during failures or malevolent acts.

The contributions of this paper are threefold: 1) it provides a tool for vulnerability assessment of power systems that is able to identify critical components and combinations of failures that have the potential to spread within the power grid, challenging the safe operation of the system; 2) it studies the progression of cascading events and system responses during single or multiple failures in the grid; 3) it provides a tool for system operators to quantify the impact of specific failures on the system operations, and thus help in the short- and long-term decision-making.

The rest of the paper is organized as follows: Section 2 describes the methodology we developed to perform the vulnerability assessment; Section 3 describes the test systems used to demonstrate the applicability of the developed methodology; The analysis and results are presented in Section 4; Finally, Section 5 presents the conclusions.

2. Methodology

The vulnerability method introduced in this paper comprises a cascading failure analysis model and a meta-heurist based optimization procedure.

2.1. *Cascading failure analysis model*

The AC power flow based cascading failure analyses model is an integral part of the Cascades platform, which is a tool for power system security assessment and transmission system expansion planning [30]. The cascading failure analyses model: simulates critical scenarios that may trigger cascading events; identifies island operations and blackout conditions; performs automatic frequency control to restore the power balance in the system; performs automatic load shedding in case of system frequency deviations beyond a safety threshold or bus voltages magnitudes below a tolerable limit; and disconnects overloaded elements (lines and transformers). One of the main objectives of the model is to reproduce the blackout/DNS statistics of a power system.

2.1.1. *Model description*

Before the cascading simulations start, the power system is in a steady state, with all components in service. To explore different loading conditions a set of power demands is selected from a yearly load curve. The generation dispatch is solved for each of the selected demands, accounting for all unit and grid constraints. Consequently, the generators supply all demand and transmission system losses, and no overloads exist. A list consisting of sets of contingencies is supplied for each demand. Each contingencies set is created probabilistically, i.e., with the Monte Carlo method. Due to discrepancies between different sources of data and to the different failure mechanism that dominate in different regions/systems, we use a single value of 0.001 for all lines and transformers. This value is based on [31]. Therefore, the majority of the contingency sets will consist of single branch failures. This concept for selection of contingencies and power demands ensures good exploration of the system conditions and in-depth assessment of the power system response under variety of possible failures. A graphical representation of the cascading failure simulation process is shown in Fig. 1.

The cascading simulation starts with the introduction of a single contingency set (initial failures). Next, islands identification check is performed after the branches comprising the contingency set are removed from the grid. The frequency deviation at each island is calculated, and based on this values two measures are envisioned (i) under frequency load shedding (UFLS), and (ii) frequency control. In the current setup, the algorithm utilizes the UFLS scheme based on the Swissgrid grid code [32], which consists of six steps. The first step is activated if the frequency deviation is lower than -0.5Hz[1], and includes the disconnection of pumped-storage hydro plants operating in pumping regime and all sources that are consuming power from the grid, e.g. transmission-scale batteries. Steps two to five are activated if the frequency deviation is between 1Hz and -2.5Hz, and load is uniformly disconnected proportional to the frequency deviation. Finally, if the frequency deviation reach -2.5Hz or +1.5Hz, all generators are disconnected. In all other cases, the frequency control employs the generating reserves to ensure load balance in the system.

The AC power flow[2] algorithm provides the line/transformer loadings and the bus voltages, which are further used for the voltage violation and line overload check (see Fig. 1). At the buses where voltage violation is detected, the under-voltage load shedding (UVLS) procedure is enforced. This is a stepwise load shedding procedure which curtails 25% of the bus load at each step until the voltage is restored within safety limits. The AC power flow calculation is repeated after each load-shedding step, updating the bus voltages and the branch loadings. The overload check is the last step of a process referred to as a cascading stage. If overload branches exist, the algorithm removes the branch with the highest flow limit violation[3], and the cascading simulation proceeds to the next cascading stage. Otherwise, the current simulation ends, and the next set of contingencies is introduced, initiating a new cascading failure simulation. The process is repeated for all sets of contingencies and all loading conditions, and then the results are assembled, processed, and presented as an output by the model.

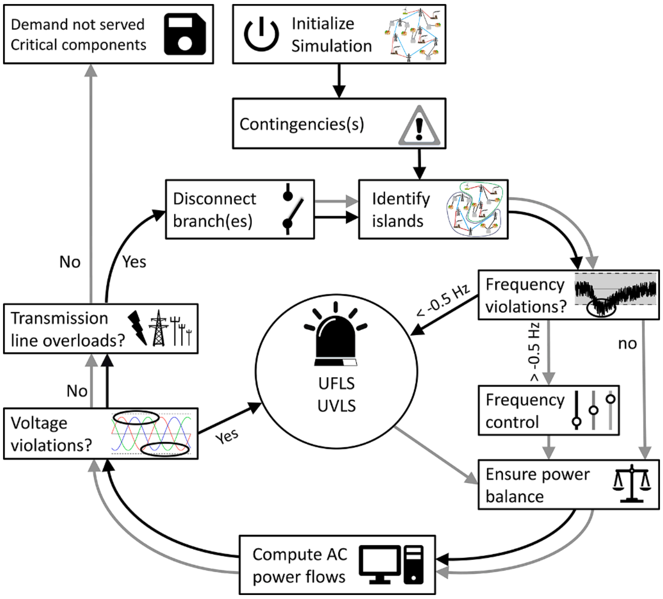

Fig. 1. A graphical representation of the cascading failure simulation process (Cascades). UFLS stands for under-frequency load shedding; UVLS stands for under-voltage load shedding.

The most relevant results of the cascading failure model is the complementary cumulative distribution function (CCDF), referred to as the risk curve[4]. Other relevant results from the cascading model include the importance/criticality of the transmission system components, the transmission system component outage occurrence, the cascading stages (the lines/transformers tripped at each stage and the corresponding DNS), and the reserves utilization.

The grid topology changes as cascade unfolds in a power grid, consequently the cascading model executes multiple AC power flows. In some occasion the AC power flow does not converge, which is a problem recognized in the scientific literature [18, 25]. The Manchester model treats this issue as a potential voltage collapse, and assumes that the operators have enough time to react and perform load shedding [18]. One of the reasons for non-convergence of the AC power flow is power system operation outside the steady state stability limits [34]. Such operation is a result of a reduced transfer capacity of the system or a lack of reactive power to supply the demand, both associated with voltage collapse conditions [35]. When the AC power flow does not converge, the Cascades model performs a steady state limits violation check by running a continuation power-flow algorithm [33, 36]. Subsequently, a set of measures are applied, including load shedding, reactive power re-dispatch, power re-dispatch, acceptance of the non-converged solution, or total system collapse. A detail description of Cascades, including the resolution of the convergence issues, and model validation, is provided in [30].

2.1.2. Criticality measures

We utilize the cascading failure simulation model to accomplish the first objective, i.e. to rank the branches in the transmission grid according to their criticality. For this purpose, the model relies on two criticality measures: (i) branch impact on DNS, and (ii) frequency of branch overload.

The cascading failure simulation model initializes with a separate list of contingencies for each of the pre-selected loading conditions. Each list consists of pre-selected number of sets of contingencies. Thus, the total number of contingency sets, i.e. the total number of cascading failure simulations is equal to the number of loading conditions multiplied by the number of contingency sets per contingency list. For each cascading simulation, the model records the DNS caused by the initial contingency set. If the set consist of more than one contingency, same amount of DNS is assigned to all of them. The process is repeated for all sets of contingencies and loading conditions and the recorded DNS is aggregated for each contingency (branch):

$$BD_k = \sum_{m=1}^{M} \sum_{n=1}^{N} DNS_{n,m}^{k} \tag{1}$$

where, BD_k is the criticality of branch k associated with the branch impact on DNS criticality measure, M is the number of loading conditions (power demands), N is the number of contingency sets per loading condition, and $DNS_{n,m}^{k}$ is the DNS assigned to branch k after performing the cascading simulations for contingency set n and loading condition m. $DNS_{n,m}^{k}$ is equal to zero in case that the cascading failure analysis do not end with DNS.

[1] The negative sign denotes frequency smaller than the nominal, while the positive sign denotes frequency larger than the nominal.

[2] For power flow calculations, the cascading failure model relies on the MATPOWER package [33].

[3] Only one overloaded branch is removed at a time.

[4] The risk curve gives the probability of observing DNS (blackout intensity) at least as extreme than the one observed.

Furthermore, the model records the frequency of branch overloads, i.e. the overloaded branches after the first cascading stage is completed (see Section 2). These overloads are important because they directly contribute to the evolution of a cascading event. The counting is performed for all sets of contingencies and loading conditions and the recorded overloads are aggregated for each branch:

$$BF_k = \sum_{m=1}^{M} \sum_{n=1}^{N} F_{n,m}^{k} \tag{2}$$

where, BD_k is the criticality of branch k associated with the frequency of branch overload criticality measure, and $F_{n,m}^{k}$ is equal to 1 if branch k is overloaded after the contingency set n is introduced into the system, otherwise $F_{n,m}^{k}$ is equal to zero.

2.2. Vulnerability identification method

To accomplish the second objective of this paper we introduce the vulnerability identification method, which aims to find the branches that if simultaneously tripped will cause the blackout with the highest intensity. In particular, we are looking for a set of two, three, or more lines/transformers that if simultaneously tripped will have the highest risk impact. The method relies on the cascading failure analysis model (Section 2.1) to assess the impact of an initial set of contingencies, and a meta-heurist based optimization procedure to explore the contingency space.

The objective function can either maximize the average DNS (DNS_{avr}) over a selected number of representable loading conditions from a yearly load curve, or find the maximum DNS over these demands (DNS_{max}). Therefore, two objective functions are defined:

$$\text{Objective function one}: \ \max(DNS_{avr}(C_{set})) \tag{3}$$

$$\text{Objective function two}: \ \max(DNS_{max}(C_{set})) \tag{4}$$

where C_{set} is a set of contingencies with a size of N_{set}, i.e. the decision variables. We decide which objective function to use and the size of the contingency set, N_{set}, before starting the vulnerability identification.

Using the objective in Eq. (3), the algorithm identifies the contingency set that results in the largest average DNS over all of the simulated hours (i.e., system loadings). Therefore, the identified contingency set is expected to have high implication to system security at any hour and any loading of the system during the year. The measures undertaken against the effects of the identified contingency set will provide an adequate level of security during most operating conditions. Using the objective in Eq. (4), the algorithm identifies the contingency set that results in the largest maximum DNS over all of the simulated hours (i.e., system loadings), i.e. the largest disruption caused by the cascading event. The identified contingency set is expected to have strong implication only for some of the yearly loading conditions and hours. The measures undertaken against the implications of the contingency set identified by Eq. (4) will provide an adequate level of security for the worst event identified by the proposed method.

The optimization procedure uses a Genetic Algorithm (GA), which is meta-heuristic optimizer capable to deal with simulation-based optimization problems as the one presented here. The flowchart of the vulnerability identification method is shown in Fig. 2. The procedure starts with a population of random solutions, *Pop*:

$$Pop = \begin{bmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,N_{set}} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,N_{set}} \\ \vdots & \vdots & \ddots & \vdots \\ c_{N_p,1} & c_{N_p,2} & \cdots & c_{N_p,N_{set}} \end{bmatrix} \tag{5}$$

where $c_{i,j}$ is the contingency, i.e. branch j to be tripped ($j = 1, 2, \ldots, N_{set}$) at solution i ($i = 1, 2, \ldots, N_p$), and N_p is the population size, i.e. the number of potential solutions. Practically, each row in *Pop* represent a single solution, which consists of integer values between 1 and the number of branches in the system.

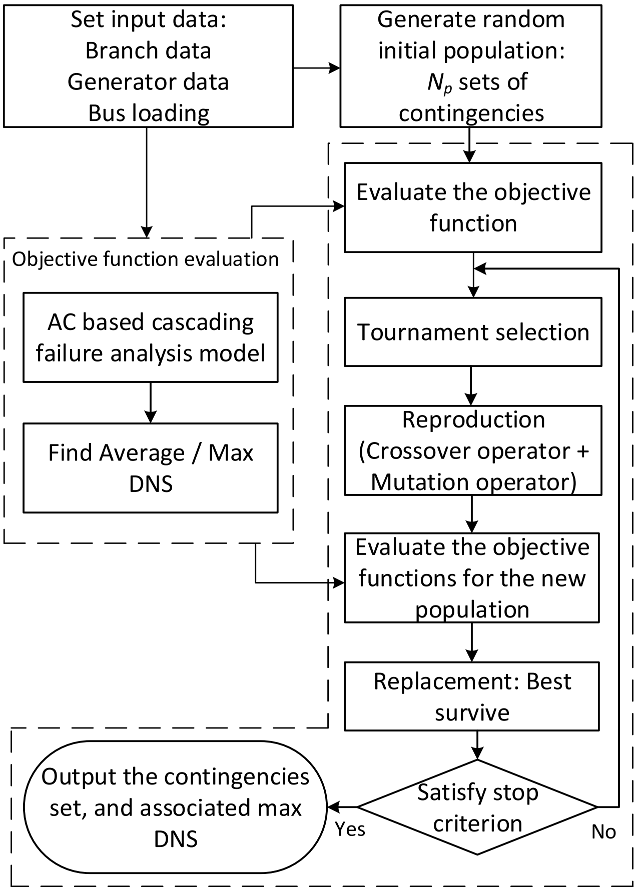
Set input data:
Branch data
Generator data
Bus loading
Generate random initial population:
N_p sets of contingencies
Evaluate the objective function
Objective function evaluation
AC based cascading failure analysis model
Find Average / Max DNS
Tournament selection
Reproduction (Crossover operator + Mutation operator)
Evaluate the objective functions for the new population
Replacement: Best survive
Satisfy stop criterion
Yes
No
Output the contingencies set, and associated max DNS

Fig. 2. Flow chart of the vulnerability identification method.

The objective function given by Eq. (3) / Eq. (4) is evaluated for each of the randomly generated solutions. The tournament selection operator is utilized to select the solutions (chromosomes) for reproduction. The selected solutions enter the reproduction step, where the blending crossover operator (BLX-α) and the non-uniform mutation operator are applied to produce the population of new solutions. The fitness of the solutions from the new (child) population is calculated and compared with the fitness of the solutions from the old (parent) population. Only the best half of the solutions survive while the rest are discarded in a process known as elitist replacement. This procedure is repeated until the maximum number of iterations is reached. A detailed description of the applied GA is given in [37].

The main output of the algorithm is the set of contingencies that results in the highest DNS with respect of the selected objective function. Furthermore, the algorithm outputs the worst cascade including the cascading stages and the DNS at each stage.

3. Test case

Two test systems are used; the IEEE 118-bus test system and Swiss power system. The 118-bus test system contains 186 branches, 9 transformers, 118 nodes and 54 generators with a combined maximum capacity of 7’200MW [38]. By default, the power demand across all load buses amounts to 3’733.07MW. This value is considered to be the mean total load over the course of a year, with the yearly load curve extracted from [39] being scaled accordingly. The one-line diagram of the IEEE 118-bus test system marking the zones in the grid is given in [38, 40]. The Swissgrid AG provides the Swiss transmission system data under an NDA agreement, including current branches and planned grid expansions up to 2025. The power plant data and power demand data are obtained from various open sources. We represent each neighboring country with a single node, e.g. all lines connecting Switzerland and Germany are connected to one representative node in Germany. Furthermore, at each of these nodes we impose the historical hourly import/export for the respective country. Due to sensitivity of the obtained results, detailed description of the vulnerabilities of the Swiss power system and the grid data are not presented in this manuscript.

The algorithm assessing grid vulnerabilities is developed in MATLAB and executed on an Intel(R) Core(TM) i9-9980XE CPU and the Euler computer cluster at ETH Zurich [41]. Calculation times vary from one to 30 hours, depending on the size of the contingency set, the population size, the number of iterations, the size of the analyzed system, and the computing machine.

4. Analysis and results

Both systems are assessed with respect to both objectives, i.e. the importance of each branch is determined, and the most critical sets of contingencies are identified.

4.1. The IEEE 118-bus test system case study

4.1.1. Criticality ranking results

The criticality ranking results for the IEEE 118-bus test system are obtained with a single run of the cascading failure model. With a list of 1000 contingency sets per loading condition and 18 loading conditions, the total number of executed cascading simulations in a single run of Cascades is 18000. Out of these contingencies, 91.1% are single branch, 8.3% are double branch, 0.5% are triple branch failures, and the remaining involve the failure of four branches or more. Fig. 3 shows branch criticality in the IEEE 118-bus test system according to the a) branch impact on DNS (Eq. (1)), and b) frequency of line overload (Eq. (2)).

Lines 8-9 and 9-10, with similar values, are the most critical components according to the branch impact on the DNS criticality measure. The failure of either of these two lines disconnects a 300 MW generator connected to bus 10. The loss of the generator causes frequency instability and results in DNS under some of the selected loading conditions. Transformer 5-8 is the third most critical component in the system according to the branch impact on the DNS criticality measure. This transformer is the main link between the generator at node 10 and the part of Zone 1 with the highest concentration of loads. Cascading failures resulting in significant DNS begin by a simultaneous failure of Line 8-9, Line 9-10, or Transformer 5-8 with other branches in the grid, in particular branches in Zone 1. Furthermore, the disconnection of Line 8-9, Line 9-10, or Transformer 5-8 initiates an overload of Line 8-30, which is the most frequently overloaded branch in the IEEE 118-bus test power system. This Line is one of the main links that connect the northern and southern part of Zone 1.

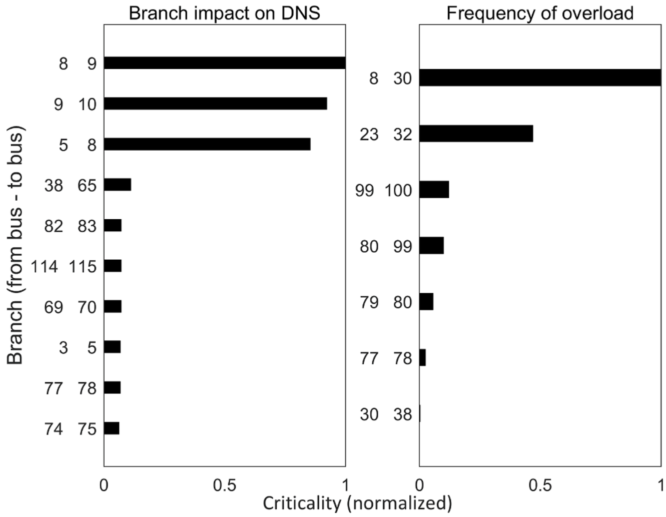

Fig. 3. Branch criticality in the IEEE 118-bus test system according to: branch impact on DNS (left), and frequency of branch overload (right).

The cascading event in Table 1 is initiate by a simultaneous failure of Lines 8-9 and 25-27 causing a chain of failures with seven stages and a DNS of 1520 MW. The disconnection of Line 8-9 results in the separation of Buses 9 and 10 from the main grid, and therefore splits the grid in two parts (islands). Buses 9 and 10 have no connected loads, and therefore the generator at Bus 10 is shutdown. The first three stages of the cascade do not result in DNS, and each stage proceed to the next with a disconnection of a single branch. The first DNS occurs at stage four and is a result of the system operating outside the steady state stability limits. This problem is resolved by uniform load shedding at all buses in the grid. Similar operating conditions occur at stages five and six, and are resolved with load shedding. Furthermore, at stage seven with the disconnection of Line 22-23 the main grid splits into two islands, where the first (smaller) island consists of most of Zone 1 and one bus from Zone 2 and the second (larger) island consist of part of Zone 1, most of Zone 2 and all of Zone 3. After the splitting, the smaller island has a frequency deviation, which is resolved with ~40 MW of load shedding. The larger island is stable and thus no additional actions are undertaken. At the end of stage seven, there are no overloads in any of the islands, and therefore the cascading simulation stops.

4.1.2. Most critical sets of contingences

To identify the sets of critical branches in IEEE 118-bus test system we run the vulnerability identification procedure described in Section 2.2. The set size for the IEEE 118-bus test system spans from two to seven contingencies, such that the algorithm is executed independently for each set size. To perform the analyses, we generate a random population of N_p contingencies for the designated set size, i.e., for a set size of two we randomly generated 90 samples of two simultaneous branch failures. Tables 2 and 3 show the sets of contingencies resulting with the worst cascades in the IEEE 118-bus test system. The Table 2 contingency sets are obtained with the average DNS based objective function (Eq. (3)), and the Table 3 sets are obtained with the maximum DNS based objective function (Eq. (4)).

Tables 2 and 3 show that some branches are participating in many of the identified contingency sets. In particular, Transformer 5-8, which is the third most critical branch according to the impact on DNS criticality measure, is part of almost all contingency sets. On the other hand, Line 8-9, which the most critical branch according to the impact on DNS criticality measure, does not show in any of the contingency sets. Whereas Line 9-10, which is the second most critical branch, only exists in the 7-branch contingency set from Table 3. This is so because in the identification of the contingency sets the algorithm is maximizing the total contribution of a set, instead of the contribution of a single component to the DNS. Furthermore, it is evident that the branches ranked according to the frequency of overload criticality measure does not show in any of the most critical contingency sets in Tables 2 and 3. This is so because the objective of the vulnerability procedure is to determine the final impact of the initial set of failures, and therefore the

Table 1
A cascading event example with all cascading stage and the DNS at each stage.

Cascading stages	1	2	3	4	5	6	7
Contingencies	8-9 25-27	23-32	8-30	17-30	33-37	19-34	22-23
DNS (MW)	0	0	0	517.22	917.94	1478.96	1520.46

Table 2
List of the most critical sets of contingencies obtained using the average DNS based objective function (Eq. 3).

Set	From Bus	To Bus	Branch type
2-branch	5	8	Transformer
	25	27	Line
3-branch	17	30	Transformer
	25	27	Line
	37	38	Transformer
4-branch	5	8	Transformer
	22	23	Line
	25	27	Line
	37	38	Transformer
5-branch	5	8	Transformer
	21	22	Line
	25	27	Line
	37	38	Transformer
	45	46	Line
6-branch	5	8	Transformer
	22	23	Line
	24	70	Line
	25	27	Line
	37	38	Transformer
	45	46	Line
7-branch	5	8	Transformer
	17	30	Transformer
	22	23	Line
	25	27	Line
	37	38	Transformer
	42	49	Line
	45	46	Line

Table 3
List of the most critical sets of contingencies obtained using the maximum DNS based objective function (Eq. 4).

Set	From Bus	To Bus	Branch type
2-branch	17	30	Transformer
	37	38	Transformer
3-branch	26	30	Line
	37	38	Transformer
	45	46	Line
4-branch	5	8	Transformer
	25	27	Line
	37	38	Transformer
	45	46	Line
5-branch	5	8	Transformer
	22	23	Line
	25	27	Line
	38	65	Line
	45	46	Line
6-branch	5	8	Transformer
	22	23	Line
	25	27	Line
	38	65	Line
	45	46	Line
	60	62	Line
7-branch	9	10	Line
	23	25	Line
	25	27	Line
	37	38	Transformer
	45	46	Line
	69	70	Line
	69	75	Line

contribution of the branches that aid the unfolding of a cascade is not directly measured. In other words, the objective functions (Eqs. (3) and (4)) are more in alignment with the impact on DNS criticality measure. A closer look of the branches given the Tables 2 and 3 shows that all of these branches are part of Zones 1 and 2, and the rest are interconnectors between these two zones. Moreover, the analysis show that simulations failure of two or more of these branches often causes overloads that frequently result in voltage and frequency instabilities, such as the event show in Table 1. Consequently, the branches that comprise the most critical set of simultaneous failures belong to Zone 1 and Zone 2 of the IEEE 118-bus test system.

Figures 4 and 5 show the average and maximum DNS per contingency set obtained using the average DNS based and maximum DNS based objective functions, respectively. Both figures show that the IEEE 118-bus test grid, with a peek demand of 6025 MW, can encounter large DNS with only two simultaneous failures. Figure 4 shows that with three and seven simultaneous failures, the average DNS is similar, i.e. the average DNS does not significantly grow with the number of simultaneous failures. Similarly, Fig. 5 shows that the maximum DNS caused by the 2-branch contingency set does not differ significantly from the maximum DNS caused by the 7-branch contingency set. Table 4 shows the cascade initiated by the most critical set of three simultaneous failures according to the maximum DNS based objective function. The DNS observed at stages two, three, and four is a result of load shedding at busses 43, 44 and 45, at which the voltage drops below the predefined limit of 0.92 p.u. At stage six, after the disconnection of Line 25-27, the system splits into two islands, where the small island consists of Buses 23, 25 and 26, and the large island represents the rest of the power system. Furthermore, at stage five, seven, and eight, the large island operates outside the steady state stability limits, which results in significant load shedding.

4.2. *The Swiss power grid test case*

4.2.1. *Criticality ranking results*

The criticality ranking results for the Swiss power system are produced with a single execution of the cascading failure model. With a list of 1000 contingency sets per loading condition and 18 loading conditions, the total number of executed cascading simulations in a single run of Cascades is 18000. Out of these contingencies, 85.1% are single branch, 13.3% are double branch, 1.5% are triple branch failures, and the remaining involve the failure of four branches or more. Figure 6 shows branch criticality in the Swiss power system according to a) branch impact on DNS, and b) frequency of line overload.

Figure 6 shows that Line 207 is the most critical component according to the branch impact on DNS criticality measure. Line 207 is an interconnector to a neighboring country that after failure during hours with high exports is causing an overload in Line 7, which is another interconnector to the same neighboring country. In most case, there are no implications of such failure to the Swiss power grid. However, in some loading conditions/exports it causes voltage violation at single Swiss node, which is resolved by the UVLS. The failure of Lines 261 and 185 is causing similar effect to the power grid. In all of these cases Line 7 overloads, which is the reason for becoming the most critical component according to the frequency of line overload criticality measure.

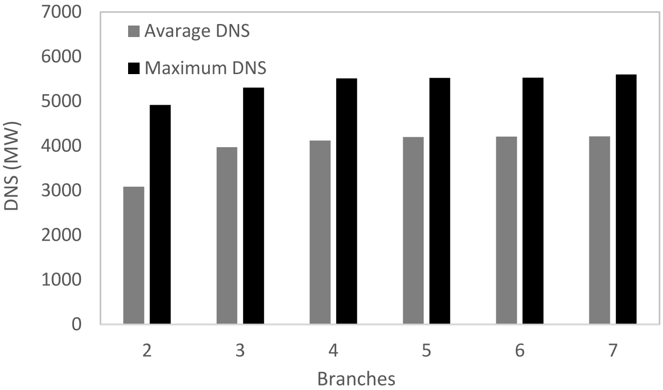

Fig. 4. The DNS as function of the sets of critical contingencies obtained using the average DNS based objective function (Eq. 3).

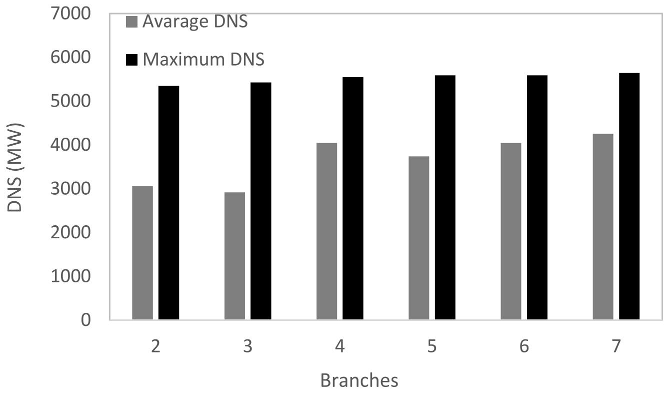

Fig. 5. The DNS as function of the sets of critical contingencies obtained using the maximum DNS based objective function (Eq. 4).

4.2.2. Most critical sets of contingences

To identify the sets of critical branches in the Swiss power system we run the vulnerability identification procedure described in Section 2.2. The set size spans from two to seven contingencies, such that the vulnerability identification is performed independently for each of them. To perform the analyses, we generate a random population of N_p contingencies for the designated set size, e.g., for a set size of five we randomly generated 1024 samples of two simultaneous branch failures. Figures 7 and 8 show the average and maximum DNS per contingency set obtained using the average DNS based and maximum DNS based objective functions, respectively. Both figures show that up to three simultaneous failures the Swiss power grid does not encounter significant blackouts. The analysis show that the recorded DNS is a result of direct disconnection of loads in the system. However, for more than three simulations failures the algorithm identifies sets of contingencies that can cause cascades with high DNS. Furthermore, the results given in Figs. 7 and 8 show that there can be significant difference between the average and the maximum DNS, especially in the case when the maximum DNS based objective function is used. This shows that at some loading conditions a contingency set can cause severe blackouts while in others the same set will have little or no effect. Furthermore, Fig. 7 shows a steady growth of the average DNS from four to seven contingencies. This is not the case when the critical contingency sets are obtained with the maximum DNS based objective function, i.e. Fig. 8 shows that the DNS is identical for the five, six, and seven most critical sets of contingencies.

5. Conclusions

The paper introduces a methodology for performing system vulnerability analysis by coupling an AC based cascading failure simulation model and a meta-heuristic based optimization procedure. The assessment provides a ranking of the individual branches according to criticality and identifies the sets of most critical failures. The applicability of the methodology is demonstrated using the IEEE 118-bus test system and the Swiss power system. The analysis of the IEEE 118-bus test system shows that the simultaneous occurrence of only two failures can result in significant blackouts. Furthermore, the sets with three to seven contingencies cause similar DNS. This DNS represents most of the power

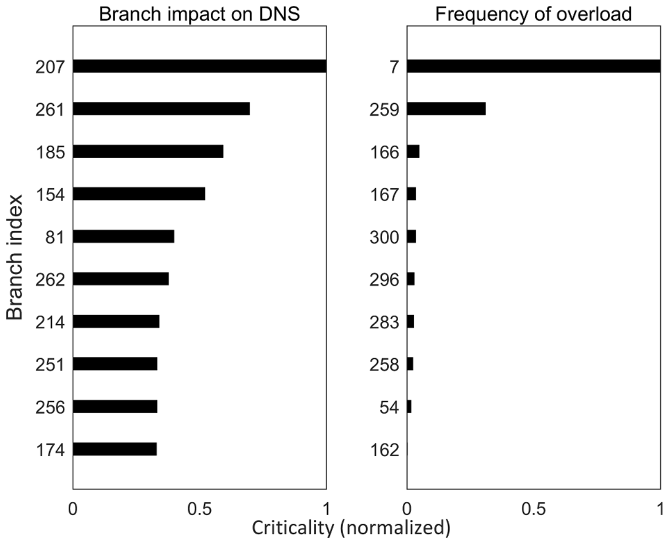

Fig. 6. Branch criticality in the Swiss power system according to a) branch impact on DNS, and b) frequency of line overload.

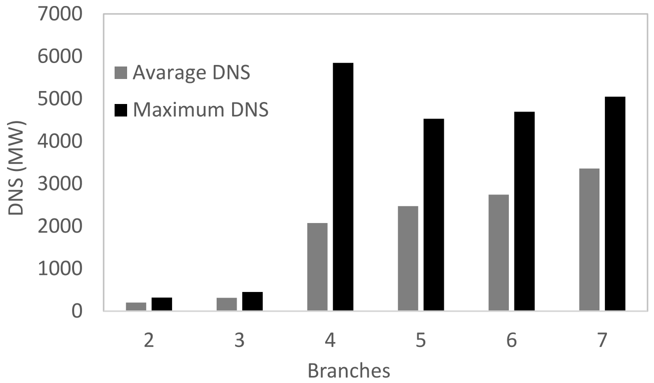

Fig. 7. The DNS as function of the sets of critical contingencies obtained using the average DNS based objective function (Eq. 3).

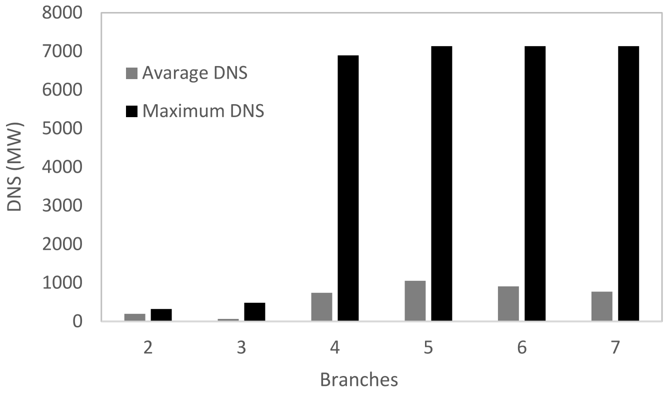

Fig. 8. The DNS as function of the sets of critical contingencies obtained using the maximum DNS based objective function (Eq. 4).

Table 4
An IEEE 118-bus test system cascading event initiated by the 3-branch failure given in Table 3.

Cascading stages	1	2	3	4	5	6	7	8
Contingencies	26-30 37-38 45-46	30-38	23-32	22-23	25-27	23-24	42-49	42-49
DNS (MW)	0	27.84	48.72	121.12	3376.97	3376.97	4037.64	5425.05

demand at the simulated loading conditions. The Swiss power system on the other hand does not encounter significant blackouts with up to three simultaneous failures. In fact, the worst DNS events with two and three simulations branch failures are a result of a direct disconnection of loads in the grid. However, with four or more simultaneous failures there are cascades that unfold and result in high DNS. Furthermore, the vulnerability identification method can reveal contingency sets that result in events with larger consequences using the maximum DNS based objective function as compared to the average DNS based objective function. Yet, these contingency sets are particularly effective for very few loading conditions and sometimes have little or no effect on the bulk of the simulated power demand conditions. Therefore, we recommend that the most attention be given to the average DNS based objective function in the development of strategies to mitigate system vulnerabilities. Such measures will be effective for the entire spectrum of loading conditions, thus providing robust protection against accidental or deliberate events. Additionally, the maximum DNS based objective function can support the identification of few scenarios leading to large consequences. Overall, the results demonstrate that the proposed method can identify weaknesses in a power system, and, therefore, the grid operators can utilize it for short and long-term operations planning and grid expansion/upgrade decisions.

CRediT authorship contribution statement

Blazhe Gjorgiev: Conceptualization, Methodology, Software, Formal analysis, Investigation, Writing – original draft, Visualization. **Giovanni Sansavini:** Conceptualization, Writing – review & editing, Resources, Supervision, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

We acknowledge the Nexus-e project: “The role of flexibility providers in shaping the future energy system” (Project Nr. SI/501460, Pilot & demonstration). This research is part of the activities of SCCER FURIES, which is financially supported by the Swiss Innovation Agency (Innosuisse-SCCER program).

References

[1] Čepin M. Assessment of power system reliability: methods and applications. London: Springer-Verlag; 2011.
[2] Murray AT, Grubesic Tony. Critical infrastructure: reliability and vulnerability. London: Springer; 2007.
[3] Abedi A, Gaudard L, Romerio F. Review of major approaches to analyze vulnerability in power system. Reliab Eng Syst Saf 2019;183:153–72.
[4] Weiss M, Weiss M. An assessment of threats to the American power grid. Energy Sustain Soc, 2019;9(1):18.
[5] Haimes YY, Horowitz BM. Modeling interdependent infrastructures for sustainable counterterrorism. J Infrastruct Syst 2004;10(2):33–42.
[6] Cuadra L, et al. A critical review of robustness in power grids using complex networks concepts. Energies 2015;8(9):9211–65.
[7] Bompard E, Luo L, Pons E. A perspective overview of topological approaches for vulnerability analysis of power transmission grids. Int J Crit Infrastruct 2015;11(1):15–26.
[8] Zio E, Golea LR, Rocco S CM. Identifying groups of critical edges in a realistic electrical network by multi-objective genetic algorithms. Reliab Eng Syst Saf 2012;99:172–7.
[9] David AE, Gjorgiev B, Sansavini G. Quantitative comparison of cascading failure models for risk-based decision making in power systems. Reliab Eng Syst Saf 2020:106877.
[10] Alipour Z, Monfared MAS, Zio E. Comparing topological and reliability-based vulnerability analysis of Iran power transmission network. Proc Instit Mech Eng Part O: J Risk Reliab 2014;228(2):139–51.
[11] Eusgeld I, et al. The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. Reliab Eng Syst Saf 2009;94(5):954–63.
[12] Bompard E, Napoli R, Xue F. Analysis of structural vulnerabilities in power transmission grids. Int J Crit Infrastruct Prot 2009;2(1):5–12.
[13] Volkanovski A, Čepin M, Mavko B. Application of the fault tree analysis for assessment of power system reliability. Reliab Eng Syst Saf 2009;94(6):1116–27.
[14] Čepin M. Probability of restoring power to the transmission power system and the time to restore power. Reliab Eng Syst Saf 2020;193:106595.
[15] Tas S, Bier VM. Addressing vulnerability to cascading failure against intelligent adversaries in power networks. Energy Syst 2016;7(2):193–213.
[16] Cheng MX, Crow M, Ye Q. A game theory approach to vulnerability analysis: Integrating power flows with topological analysis. Int J Electr Power Energy Syst 2016;82:29–36.
[17] Carreras BA, et al. Critical points and transitions in an electric power transmission model for cascading failure blackouts. Chaos: Interdiscip J Nonlinear Sci 2002;12(4):985–94.
[18] Nedic DP, et al. Criticality in a cascading failure blackout model. Int J Electr Power Energy Syst 2006;28(9):627–33.
[19] Li J, et al. AC power flow importance measures considering multi-element failures. Reliab Eng Syst Saf 2017;160:89–97.
[20] Fang Y-P, Sansavini G, Zio E. An optimization-based framework for the identification of vulnerabilities in electric power grids exposed to natural hazards. Risk Anal 2019;39(9):1949–69.
[21] Liu X, Fang Y-P, Zio E. A hierarchical resilience enhancement framework for interdependent critical infrastructures. Reliab Eng Syst Saf 2021;215:107868.
[22] Beyza J, Yusta JM. The effects of the high penetration of renewable energies on the reliability and vulnerability of interconnected electric power systems. Reliab Eng Syst Saf 2021;215:107881.
[23] Abedi A, Gaudard L, Romerio F. Power flow-based approaches to assess vulnerability, reliability, and contingency of the power systems: The benefits and limitations. Reliab Eng Syst Saf 2020;201:106961.
[24] Henneaux P, et al. Benchmarking quasi-steady state cascading outage analysis methodologies. In: 2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS); 2018.
[25] Eppstein M, Hines P. A “Random Chemistry” algorithm for identifying collections of multiple contingencies that initiate cascading failure. In: 2013 IEEE Power & Energy Society General Meeting; 2013.
[26] Rocco CM, et al. Assessing the vulnerability of a power system through a multiple objective contingency screening approach. IEEE Trans Reliab 2011;60(2):394–403.
[27] Donde V, et al. Severe multiple contingency screening in electric power systems. IEEE Trans Power Syst 2008;23(2):406–17.
[28] Haes Alhelou H, et al. A survey on power system blackout and cascading events: research motivations and challenges. Energies 2019;12(4):682.
[29] Andersson G, et al. Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance. IEEE Trans Power Syst 2005;20(4):1922–8.
[30] Gjorgiev B, et al. Cascades Platform. Reliability and Risk Engineering (RRE) Zurich; 2019.
[31] Yang S, et al. Failure probability estimation of overhead transmission lines considering the spatial and temporal variation in severe weather. J Modern Power Syst Clean Energy 2019;7(1):131–8.
[32] Swissgrid, Transmission Code 2013. 2014.
[33] Zimmerman RD, Murillo-Sanchez CE, Thomas RJ. MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education. IEEE Trans Power Syst 2011;26(1):12–9.
[34] Ajjarapu V, Christy C. The continuation power flow: a tool for steady state voltage stability analysis. IEEE Trans Power Syst 1992;7(1):416–23.
[35] Feng Dong TK, Lam Baldwin. Dealing with power flow solution difficulties. Power Technology. Siemens Energy, Inc; 2012.
[36] Hsiao-Dong C, et al. CPFLOW: a practical tool for tracing power system steady-state stationary behavior due to load and generation variations. IEEE Trans Power Syst 1995;10(2):623–34.
[37] Gjorgiev B, Čepin M. A multi-objective optimization based solution for the combined economic-environmental power dispatch problem. Eng Appl Artif Intell 2013;26(1):417–29.
[38] IIT. "*http://motor.ece.iit.edu/Data*" Illinois Institute of Technology, Electrical and Computer Engineering Department, [Online]. 06.08.2019].
[39] USEIA. U.S. Electric System Operating Data. *https://www.eia.gov/realtime_grid/#/data/graphs?end=20170108T00&start=20170101T00&regions=04*. 06.08.2019].
[40] Peña I, Martinez-Anido CB, Hodge B. An Extended IEEE 118-Bus test system with high renewable penetration. IEEE Trans Power Syst 2018;33(1):281–9.
[41] ETHZ. Euler - Scientific computing. 2020 [cited 2020 03.03]; Available from: https://scicomp.ethz.ch/wiki/Euler.