Reliability Engineering and System Safety 201 (2020) 106950

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Security assessment of cross-border electricity interconnections

Jesus Beyza[a,b], Pablo Gil[b], Marcelo Masera[c,*], Jose M. Yusta[b]

[a] Instituto Tecnologico de Morelia, PGIIE, Avda. Tecnologico 1500, 58120, Morelia, Mexico
[b] Universidad de Zaragoza, Departamento de Ingenieria Electrica, C/Maria de Luna 3, 50018, Zaragoza, Spain
[c] Energy Security, Distribution and Markets Unit, Directorate of Energy, Transport and Climate, Joint Research Centre, Petten 1755 LE, The Netherlands

ABSTRACT

Cross-border electricity interconnections are important for ensuring energy exchange and addressing undesirable events such as power outages and blackouts. This paper assesses the performance of interconnection lines by measuring their impacts on the main reliability and vulnerability indicators of interconnected power systems. The reliability study is performed using the sequential Monte Carlo simulation technique, while the vulnerability assessment is carried out by proposing a cascading failures methodology. The conclusions obtained show that highly connected infrastructures have simultaneously high reliability and limited robustness, which suggests that both approaches show different operational characteristics of the power system. Nevertheless, an appropriate increase in the number and capacity of the interconnections can help to improve both security parameters of the power supply. Seven case studies are performed based on the IEEE RTS-96 test system. The results can be used to help transmission system operators better understand the behaviour and performance of electrical networks.

1. Introduction

Power systems are increasingly large and complex due to the rapid development of modern societies, which have created innumerable challenges of analysis for infrastructure operators. This prolific growth has been accompanied by the construction of new plants and assets to maintain the levels of reliability and security of the electricity grid. More recently, in the member countries of the European Union, this progress has also included improvements in cross-border electricity interconnections to increase the electricity supply and integrate more renewable energy sources into the energy markets [1]. The merging of two or more electricity infrastructures has created numerous benefits for the economy and the population, since a country can rely on neighbours for importing the necessary electricity and becoming better equipped to manage undesirable events, such as weather events, failures and blackouts. Additionally, the need to build new power plants is reduced, and the optimal management of renewable energies is facilitated, among many other factors [1–3]. Therefore, connecting isolated power systems is essential for supply security.

In the case of coupled electrical infrastructures, a failure within one of the systems has the potential to propagate throughout the network. For example, the European blackout in 2006 was due to a routine disconnection of a single power line in northwest Germany, which caused more than 15 million customers in five countries of the Union for the Coordination of the Transmission of Electricity (UCTE) to be without electricity for approximately two hours [4]. These critical infrastructures must operate safely and reliably.

These aspects highlight the importance of managing these risks and vulnerabilities. Traditionally, the risk management approach that ensures proper operating conditions of electrical infrastructure has prevailed since it identifies the most potential threats and hazards. However, in risk management, two complementary approaches can be considered - high-probability but low-impact events or low-probability but high-impact events [5–7]. The first class of events corresponds to the reliability approach, since it considers n-1 and n-2 contingencies, while the second class of events corresponds to the vulnerability approach since it considers n-*k* contingencies [8].

This article considers that both perspectives of risk analysis should be integrated within a unified decision framework to compensate for the limitations of a single approach in the study of cross-border interconnections. The reliability analysis, as the focus of risk management in power networks, should be complemented with a vulnerability analysis to improve the planning of the system's expansion and better understand the structural performance of the networks. Feeder links can improve the levels of reliability but fail to achieve improvements in the levels of vulnerability, or they can improve the vulnerability but simultaneously worsen the reliability. In these situations, the construction of new connecting lines must consider both approaches to improve the performance and behaviours of the interconnected systems.

Reliability can be defined as the capacity of the power system to continuously satisfy demand with an acceptable level of quality or perform a required function in given environmental and operational conditions for a given period [9–12]. Other similar definitions are provided in [13, 14]. Several approaches can be employed to conduct

[*] Corresponding author.
E-mail address: Marcelo.MASERA@ec.europa.eu (M. Masera).

https://doi.org/10.1016/j.ress.2020.106950
Received 20 September 2019; Received in revised form 19 February 2020; Accepted 23 March 2020
Available online 11 May 2020
0951-8320/ © 2020 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license
(http://creativecommons.org/licenses/BY/4.0/).

reliability studies, from analytical models to Monte Carlo probabilistic models. The latter is a more flexible methodology than analytical models but requires more calculation time, especially when operating conditions and complex system states are considered. The reliability of electrical infrastructure is measured in terms of the indices presented in Section 3.

Reliability assessments are based on the probabilistic estimation of the failures and the negative quantification of these events or incidents [15–17]. These estimates are purely quantitative since they are constructed considering the estimated probabilities, which can generate some uncertainty in the final results [18, 19]. Some authors argue that risk management should also incorporate concepts such as robustness and resilience to further improve the security of power networks [15, 18]. In this sense, the vulnerability approach is the methodology with the best characteristics to address these concepts.

Vulnerability is the degree with which an electrical network degrades due to a loss of functioning of its elements after an attack or failure [20, 21]. Vulnerability can also be defined as the inability of an infrastructure to withstand variations in voltages and the effects of failures [22]. The term robustness, complementary to the term vulnerability, is used to define the ability of a system to maintain, at least partially, the electrical supply in the case of unforeseen events or incidents [23]. For example, the single interruption of a transmission line can cause the overload of other lines, which increases the likelihood that other assets will fail and cause a system-wide failure [24]. Unlike the reliability approach, the vulnerability approach does not consider the probabilities of failures or threats but rather quantifies the effect or impact of the disturbances on the structural performance of the network to identify potential threats. Vulnerability is an inherent characteristic of power systems.

Few documents discuss the two approaches, and the results are contrasted in parallel [25–27], that is, systematic comparisons to identify how the two approaches can be applied in a complementary manner are lacking.

This article addresses the lack of comparative studies analysing the impact of cross-border interconnections with reliability and vulnerability assessment approaches. The objective is to show, using empirical evidence, that feeder links have an important role in supply security but simultaneously have the potential to cause disturbances in a joint network since they can propagate failures or disruptions [2]. The network selected to carry out this study is based on the well-known IEEE RTS-96 test system, from which seven different case studies are extracted [28]. This system is chosen as it is a sufficiently small network for performing a large number of studies with a reasonable solution time but sufficiently detailed to reflect the actual complexities involved in reliability and vulnerability approaches. This system includes main generation and transmission facilities in a simple but representative model of real interconnected infrastructures. The premise is to illustrate, as much as possible, different technologies and configurations in power systems [28].

Two studies are executed using the procedures and provisions identified in their respective fields of research. The reliability approach is performed using the sequential Monte Carlo simulation technique, and the vulnerability approach is executed using a cascading failure procedure [29–31]. The discussion seeks to enrich the scientific debate by demonstrating that results from the reliability and vulnerability analyses can be combined and discussed in parallel and show how these approaches can provide complementary information about the interconnected infrastructure.

The remainder of this document is organised as follows: Section 2 provides a review of the most representative documents of the reliability and vulnerability approaches. Section 3 describes the procedures for evaluating the reliability and vulnerability of interconnected power systems. Section 4 presents the case studies based on the IEEE RTS-96 test network and separately shows the numerical results of reliability and vulnerability. Section 5 discusses the findings jointly, and Section 6 summarises the main conclusions of this work.

2. Reliability and vulnerability approaches

This section presents some important characteristics of the reliability and vulnerability studies of power systems. These characteristics, although not exhaustive, describe the fundamental principles involved with each technique.

2.1. Evaluation of reliability

Reliability is the ability of a power grid to operate at the required level of quality over a long period. The most analysed contingency events are those that correspond to n-1 and n-2, which represent the loss of one or two infrastructure assets, respectively. Reliability is broken down into system adequacy and system security [14, 32]. System adequacy evaluates whether the capacity of energy generation is adjusted to the demand and the limitations of the network in stable conditions without contingencies. System security analyses the behaviour and performance of a network against the nontrivial loss of a generator or transmission line. The purpose of the reliability analysis is to describe the behaviour of the network and calculate indices that describe intrinsic characteristics, such as energy not supplied, demand not supplied, unmet demand, among others [13, 15]. The study performed in this article focuses on the security of the system as related to the performance of the interconnected network.

This type of evaluation can be performed from an analytical or simulation perspective. The analytical technique represents the infrastructure via analytical models and evaluates the indices using mathematical solutions. This approach requires assumptions to simplify the problem and produce an analytical model of the network so that the resulting analysis may lose some or much of its meaning. The solution using this technique is obtained in a relatively short time [14, 33, 34]. The Monte Carlo simulation technique estimates the reliability indicators that simulate the process and random behaviour of the network via experiments. Theoretically, this approach can take into account all of the aspects and contingencies inherent to the planning, design and operation of the infrastructure. These aspects include random events, such as power outages and repairs of components constructed from general probability distributions, component behaviours and power variations [33, 34]. In general, the analytical technique is efficient when the operating conditions are not complex, or the probability that assets will fail are quite slim, and the Monte Carlo technique is preferable for complex operating conditions or a large number of events. This latter approach is employed in this study for the reliability analysis of the proposed case studies [33].

A reliability analysis based on the Monte Carlo simulation approach generally employs two techniques: sequential and non-sequential. On the one hand, the sequential technique simulates the real chronological process and the random behaviour of the electrical infrastructure [33, 34]. This technique is performed by dividing the simulations into periods and considering the contingencies produced in each case. The sets of events are directly related to the previous simulation conditions. The indicators are quantified when interruptions over one year are considered [15, 20]. On the other hand, the non-sequential technique samples the system in such a way that each time step, system state or failure event is considered independently, which produces a non-chronological network state, i.e., less realistic state [33, 34]. This research applies the sequential Monte Carlo simulation technique since it is a more flexible and precise approach than the non-sequential technique in addition to representing a more realistic behaviour of the coupled infrastructure.

2.2. Evaluation of vulnerability

The vulnerability of the power system has been a well-studied area of research in the last decade. Despite being a common term, more than twenty definitions of this concept are provided in the scientific literature [35]. Some authors suggest that vulnerability can involve social, organisational, economic, environmental, territorial, physical and systematic aspects [36]. However, the majority of studies focus on systematic and physical vulnerabilities [36]. For this article, vulnerability is an internal characteristic of electrical systems that is related to the inability to withstand the effects of failures [37].

Vulnerability can be studied in two different ways: functional vulnerability and structural vulnerability. Functional vulnerability is related to the operational aspects and conditions of infrastructure, while structural vulnerability is related to a decrease in the performance of a network after a failure or event. For more information, consult [38]. The study of the impact of cross-border interconnections in interconnected power systems is carried out from the perspective of structural vulnerability, as it evaluates the combined performance of networks when they are subject to multiple n-*k* contingencies, i.e., cascading failures. The initial hypothesis of this study suggests that cross-border connections can cause a decrease or drop in total network performance as disturbances can propagate through these lines.

The assessment of vulnerability has many objectives according to the uses of the researchers, such as identifying the critical components that require protection, determining possible undesirable events, classifying the components according to their consequences, identifying potential vulnerabilities, identifying existing countermeasures and estimating the degree of vulnerability of each component [14, 36, 39, 40]. This type of study, unlike the study of reliability, does not consider the probabilities of failure of the elements; instead, it exhaustively quantifies the impact caused in the topology by the systematic removal of the assets. Contingency studies are among the criteria most employed to evaluate the degree of impact of an event [41].

2.3. Discussion

Reliability and vulnerability studies of power networks are well-documented approaches in the scientific literature. However, the security evaluation of cross-border interconnections in interconnected electrical systems is a recent area of research with a lack of studies that address both concepts in parallel. As a result, this study seeks to contribute to bridging the gap to the apparent lack of related studies in this field of research.

Interconnected electrical infrastructures are operated by different independent Transmission System Operators (TSOs), who may unintentionally perform actions that could damage network operation. Therefore, the exchange of information should be considered when analysing the joint vulnerability and reliability of networks [42].

The coupling of systems with different operational or topological characteristics can drastically increase the joint vulnerability of the networks, although from the point of view of reliability, improvements are possible [43, 44]. For example, when two infrastructures of different sizes are coupled, larger networks may be less vulnerable than small networks when few interconnections exist due to less propagation of the disturbances of the other joint systems. Meanwhile, small networks can be more vulnerable than large networks when many interconnections exist due to the substantial difference in the scale of the systems. Conversely, the interconnected systems would be much more reliable from a reliability approach since the infrastructures would be less sensitive to power outages caused by a malfunction. Both situations shown here can compromise the coupling of power networks.

Vulnerability studies with the potential to identify and classify the most severe failures or impacts can serve as a technique to determine and optimise the best feeder links, improve the coupling of infrastructure and mitigate undesirable events [45, 46].

Another essential aspect of recent consideration in the security of interconnected systems is the constant occurrence of cyberattacks against control systems. Vulnerability studies identify assets whose destruction or weakening present an extremely high risk to the coupled system [47, 48]. This approach also helps measure the evolution of interconnected networks both before and after contingency events [49, 50]. In scientific literature, several traditional techniques for carrying out these tasks are identified [51–53].

The combined analysis of the results of the reliability and vulnerability studies can offer a new perspective for evaluating the security of cross-border interconnections since the information generated by both approaches enables us to improve the understanding of these links. This article provides new knowledge in this area of research.

3. Procedure to quantify the impacts of interconnections on reliability and vulnerability

This section describes the methodology and statistical indicators used to study the impact of cross-border interconnections on the reliability and vulnerability of coupled systems.

3.1. Methodology for the reliability calculation

The study of reliability requires the calculation of statistical indicators to measure the efficiency of the electrical infrastructure. The computation of these indicators is based on the frequency, duration, and magnitude (or the probability) of adverse effects on the electric supply. Regarding the security dimension of reliability, n-1 security principle is usually employed [54]. This analysis aims to prevent emergency conditions in the power grid, including the propagation of incidents from one system to another [54]. Failure events are statistically independent, as asset disruptions are not related to other contingencies occurring in another location in the network. This simulation process realistically takes into account all aspects inherent in the design and operation of the infrastructure. In this regard, TSOs have a variety of indexes that allow them to measure the severity of a disruptive event and to establish effective mitigation measures.

To calculate the security indicators, the sequential Monte Carlo technique has an orderly procedure of steps that can be summarised as follows [33, 34]:

Step 1. Determine the status of components susceptible to failures. The two possible states of the assets of an electrical network are normal or failure. Initially, all assets are assumed to be in a normal state.
Step 2. Calculate the time the components spend in each state. The time to failure (TTF) and time to repair (TTR) are calculated sequentially using the failure rates (λ), uniformly distributed random numbers between [0,1] (r) and mean time to repair (MTTR) using equations (1) and (2), respectively. The r-values are calculated using congruential generators [33].

$$\mathrm{TTF} = -\frac{\ln(r)}{\lambda} \times 8760 \tag{1}$$

$$\mathrm{TTR} = -\ln(r) \times \mathrm{MTTR} \tag{2}$$

This step is repeated for a specific amount of time, usually one year.

Step 3. Provide the overlap times of the failures for an annual horizon with an hourly resolution (8760 steps).
Step 4. Run optimal power flow study after a failure in the assets.
Step 5. Measure the reliability indicators in equations (3) through (8) using the load flow results from step 4.

Expected energy not supplied [MWh/year]

$$\text{EENS} = \frac{\sum_{i=1}^{N_y}\sum_{j=1}^{N_i} E_{j,i}}{N_y} \tag{3}$$

where $E_{j,\ i}$ is the energy not supplied (MW) to the electrical network in the j-th power interruption in year i, N_y is the total number of years simulated and N_i is the total number of interruptions in year i.

- Expected demand not supplied [MW]

$$\text{EDNS} = \frac{EENS}{8760} \tag{4}$$

- Expected Frequency of Load Curtailments [outages/year]

$$\text{EFLC} = \frac{\sum_{i=1}^{N_y} N_i}{N_y} \tag{5}$$

- Loss of load expectancy [hours/year]

$$\text{LOLE} = \frac{\sum_{i=1}^{N_y}\sum_{j=1}^{N_i} D_{j,i}}{N_y} \tag{6}$$

where $D_{j,\ i}$ is the duration of the j-th power interruption in year I (hours).

- Loss of load probability [%]

$$\text{LOLP} = \frac{LOLE}{8760} \tag{7}$$

- Loss of load duration [hours/disturbance]

$$\text{LOLP} = \frac{LOLE}{8760} \tag{8}$$

Step 6. Repeat the previous steps until the EENS covariance index is less than a predefined tolerance.

It should be noted that it is possible to take into account statistical uncertainty in the input data when calculating the above indicators. For this purpose, different probability functions associated with component failure and restoration activities can be used. The objective is not only to calculate reliability indices in the form of expected values of random variables, but also the distributions of these indices. The most commonly used probability distributions are Weibull, normal and log-normal [55]. This modified approach assumes that the components have the same adjacent distribution and that the failure and repair processes of the assets follow exponential distributions [56].

3.1.1. Plexos software

The Plexos software was used to develop the reliability studies in the proposed cases, quantify the statistical indexes presented in the previous point, and measure the impact of cross-border interconnections on the reliability of electrical networks. Plexos is a tool used to model and plan electricity and gas markets that is widely used by the Energy Regulatory Commission (ERC) of Ireland and the California Independent System Operator (CAISO), among many other public and private organisations [29, 57, 58]. This software can calculate the reliability indices of LOLP, LOLE, EDNS and EENS from the PASA simulation phase using convolution. However, it can also use the detailed chronological simulation of ST Schedule to produce the same indicators using Monte Carlo [59]. This latter approach is used in this article. Although Plexos is a well-known software for conducting reliability studies, this subsection illustrates the applicability of the program as an accurate and efficient modelling tool.

Table 1
Comparison of the reliability results.

Index	Reference [25]	Reference [32]	This article
Demand (MW)	2,850	2,850	2,850
EENS (MWh/year)	127,546	134,590	130,591
EENS (%)	0.51	0.54	0.52
EDNS (MW)	14.56	15.36	14.91
EFLC (outages/year)	18.8	18.57	18.59
LOLE (hours/year)	732	740.22	764.62
LOLP (%)	8.3	8.45	8.73
ADLC (hours/outage)	38.8	39.86	41.13

For the case study, the well-known IEEE RTS-96 test network was selected; its technical and operational characteristics are described in detail in Appendix A [28], and the software was configured to perform 500 iterations using the sequential Monte Carlo technique with a preset tolerance of 1.5%. The simulation data for each area can be found in [15]. The results were compared with those reported in references [25] and [32]. The programme was run on a personal computer with an Intel® Core™ i5, 1.80 GHz CPU and 6 GB RAM. The simulation time was 8.43 hours.

Table 1 contains the results of the reliability indicators obtained in this article in comparison with the results shown in references [6] and [26]. As can be seen, the results calculated with the Plexos program compare well with those reported in the references, indicating that the model used provides results similar to those calculated with the traditional methods already known. This shows that the functional model can be applied to the case studies presented in the following section.

3.2. Methodology for the vulnerability calculation

Structural vulnerability evaluates the physical characteristics of the topology of the infrastructure when subjected to various n-k contingencies. The aim is to prove whether cross-border interconnections cause a decrease in network performance when disruptions propagate through these links to the other interlinked systems.

3.2.1. Vulnerability metric

The appraisal of the performance of the interconnected infrastructures is done through an index that quantifies the power supply during the disintegration process. Similar to other studies [60–62], the load shedding (LS) indicator is used to determine the effect of cascading failures on the coupled network. The contingencies considered correspond to random events such as component failures, protective devices malfunctions, and human errors [63]. In this paper, cascading failures are successive events of faults in the system's elements, even if the failed assets are not adjacent.

The LS index is calculated as follows:

$$LS = \frac{\sum_i P_{Di}^{LC}}{\sum_i P_{Di}^{BC}} \tag{9}$$

where P_{Di}^{LC} is the power load that remains electrically connected, following a node i disruption (MW), and P_{Di}^{BC} is the power load under the base case (MW).

The LS metric varies between 1 and 0. Therefore, as the LS index decreases or approaches zero, the impact on the entire infrastructure increases. To calculate LS, a DC optimal power flow (DCOPF) study was used, which considered the active power as the most important parameter [64].

3.2.2. Structural vulnerability algorithm

Algorithm 1 quantifies the impact of interconnections on interconnected power systems subject to multiple correlated n-k contingencies. The procedure incorporates equation (9) depending on the assets or elements eliminated. The algorithm begins by running a DCOPF study to determine the total active power under the base case and setting the LS index to 1, since $P_{Di}^{LC} = P_{Di}^{BC}$. Contingency events are simulated by randomly eliminating buses and changing the topology after each disruption. Due to the random nature of the results, a threshold of experimental samples (Δ) is required to obtain an adequate statistical sample, as reported in [65]. For each system studied, 1000 result samples were considered.

In addition, the bus removed is never the slack bus. This bus is not removed because it is responsible for providing energy balances in the flow equations. Although other buses can be chosen as references, this is not done because the objective is to have a single measurement network. The reason for this is that islands are generated during the process of disintegrating the grid; therefore, it is necessary only to select the subnet containing the slack bus. Algorithm 1 uses the Depth First Search (DFS) algorithm to determine the islands in the network [66]. Then, DCOPF is only executed on the selected subnet to determine the active power load that remains electrically connected, following the removal of node i, i.e., P_{Di}^{LC}. The algorithm ends when no more assets can be removed or if the sample threshold is reached.

4. Case studies

This section presents the case studies constructed from the IEEE RTS-96 test network, from which seven different interconnected networks were extracted [28]. The reliability and vulnerability results for each system studied are also reported.

4.1. Description of the case studies

The IEEE RTS-96 system is a good case study because it represents, in real terms, a coupled infrastructure consisting of three identical power systems [28]. Each electrical network consists of 24 buses, 32 generators and 38 power lines and transformers. This study considers a failure rate of 0.001/year, a 24-hour MTTR and an annualised peak power demand of 2850 MW in each infrastructure [15]. The technical data of the network can be consulted in Appendix A [28].

This system has three equal areas that are connected as follows: Area 1 is connected to Area 2 by three power transmission lines, Area 2 is connected to Area 3 by a transmission line, and Area 3 is connected to Area 1 through an additional bus, an electric transformer and a transmission line.

For simulation purposes, only Areas 1 and 2 (herein called Areas A and B) with their three respective interconnecting links were considered, as shown in Fig. 1. By alternately combining the three interconnectors, seven different networks were extracted for analysis.

In isolated power systems, load shedding can occur when generation does not meet the load demand. In interconnected power systems, this deficiency can be met by exchanging power from other systems. This support depends on the available capacity, the operational reserve, the interconnection constraints and the type of agreement between the infrastructures. That is, the capacity of the tie lines imposes limits on assistance from one system to another — the above factor impact on the reliability levels of the interconnected systems. Table 2 shows the systems studied, the interconnection lines considered, and the capacities of the interconnection lines.

It should be noted that Network 1 consists of Areas A and B connected with transmission lines[23-17],[13-15] and [07-03]. Network 2 also consists of Areas A and B, but they are connected with links [23-17] and [13-15]. Networks 3 and 4 also connect the two areas with two of the possible lines, while Networks 5 to 7 each use a single interconnector.

4.2. Effect of interconnections on reliability

Table 3 shows the reliability results of the different networks studied using the Plexos software. Five hundred iterations are considered for each system and covariance of less than 2%. Figure 2 shows the convergence results of the EENS index when the sequential Monte Carlo simulation technique is applied.

The results in Table 3 show that reliability improves as the number of links between the systems increases. The best-case corresponds to the interconnection of the two areas with three power lines (Network 1), where the reliability improves by 71% compared to the isolated grid.

The values of the EENS metric (%) are better in the case of the interconnected areas of the first six case studies, where small improvements are seen between the cases of Networks 1 to 6 as the number and capacity of the interconnections increase. Thus, the minimum EENS value is 0.151% in Network 1 compared to 0.164% in Network 6.

However, the EENS is more than two times higher in the case of the grid-connected with the line with the lower capacity [07-03] (Network 7) than in the other cases. Nevertheless, when the results of the system for case 7 are compared with those shown in Table 1, which correspond to an isolated grid, EENS decreases from 0.52% to 0.35%, which indicates that a single interconnection line has the potential to improve the reliability. The LOLP and LOLE indices have similar results.

Interconnections have an important role because they serve as support elements between the different areas that make up an interconnected system. The efficient use of these connections is related to the power that they can transmit to the joint systems. It is therefore proposed to study this feature using the indicators of exchanged energy (EE), maximum percentage of line capacity (MPLC) and percentage of exchanged energy (PEE):

■ Exchanged energy [MWh/year]

$$\mathrm{EE} = \frac{\sum_{i=1}^{N_y} \sum_{j=1}^{L} \sum_{k=1}^{8760} F}{N_y} \tag{10}$$

where N_y is the total number of years simulated, L is the total number of interconnections lines between areas, and F is the active power.

■ Maximum percentage of line capacity [%]

$$\mathrm{MPLC} = \frac{\mathrm{MLC}}{\mathrm{NTC}} \times 100 \tag{11}$$

where MLC is the maximum line capacity (MW) and NTC is the net transfer capacity (MW).

■ Percentage of exchanged energy [%]

$$\mathrm{PEE} = \frac{\mathrm{EE}}{\text{Annual demand}} \times 100 \tag{12}$$

These metrics are important for describing the contributions of the connections. Table 4 shows the line loading of the interconnections for the seven grids studied. It should be noted that Network 1 has the highest annual PEE indicator, which implies that the use of the interconnections between highly connected grids is high. This means that the higher the interconnection capacity is, the greater the power exchange between areas is. This benefits the systems because it facilitates mutual support in case of contingencies.

Additionally, the EE results in Table 4 show that Area B strongly supports Area A in all of the systems studied, which could be due to the technical characteristics of the assets that work as an interconnection. Furthermore, the MPLC results indicate that the capacity of the interconnection lines is sufficient: the busiest line corresponds to link [07-03] in the case study of Network 7, which has an annual maximum utilisation of 47.89% of its capacity, and the average of the remaining lines is approximately 25%.

In short, interconnections increase the reliability of interconnected

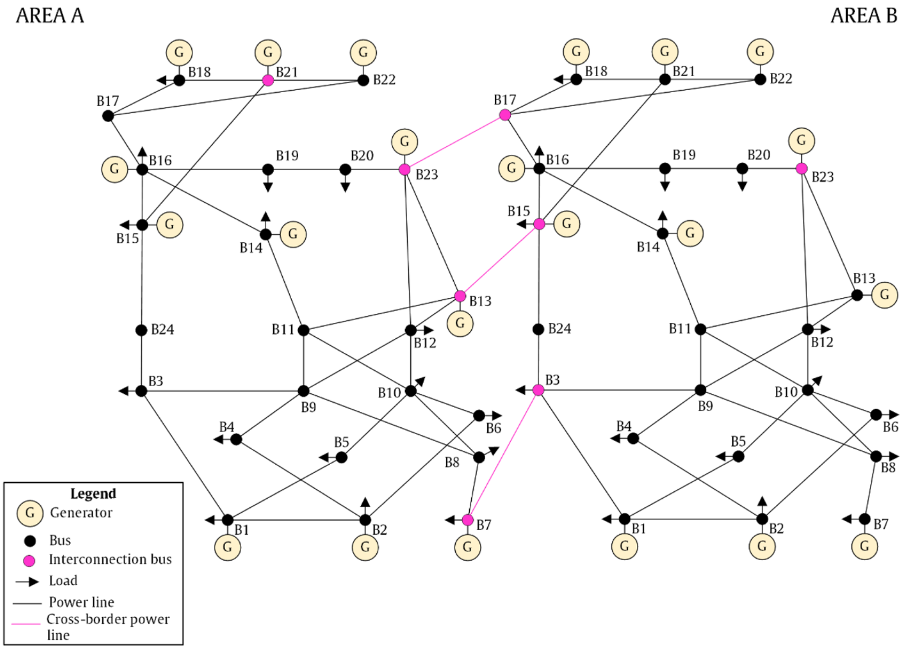

Fig. 1. Diagram of the IEEE RTS-96 test network.

Table 2
Topology and characteristics of the case studies.

Case studies	Interconnection lines	Capacity of the interconnection lines (MW)
Network 1	[23-17], [13-15] y [07-03]	608 + 608 + 208 = 1424 MW
Network 2	[23-17] y [13-15]	608 + 608 = 1216 MW
Network 3	[23-17] y [07-03]	608 + 208 = 816 MW
Network 4	[13-15] y [07-03]	608 + 208 = 816 MW
Network 5	[23-17]	608 MW
Network 6	[13-15]	608 MW
Network 7	[07-03]	208 MW

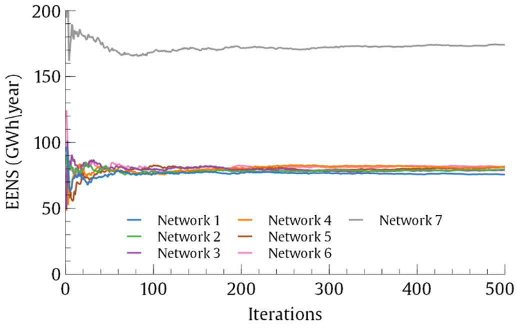

Fig. 2. Convergence of the Expected Energy Not Supplied (EENS) index.

systems; however, the capacity of the links in the energy exchange and the buses or assets selected as interconnecting elements should always be considered.

4.3. Effect of interconnections on vulnerability

According to the methodology described in Section 3.2, the disintegration of the systems was carried out by introducing random failures and calculating the LS statistical indicator during the disintegration process. The results were obtained by averaging 1000 simulation samples for each infrastructure studied. When all of the buses are initially connected, the LS index is equal to 1. Then, as the grid disintegrates due to the propagation of cascading failures, the LS index decreases to 0, which means that the power supplies to all loads on the grid have been interrupted. Figure 3 shows the performances of the seven interconnected networks under cascading failures and the vulnerability curve of a separated Area A.

The results show that Area A initially collapses with the removal of approximately 80% of the buses. In the remaining cases, the grids disintegrate more quickly because the removal of 60-70% of the buses is more than sufficient to cause a widespread blackout. Furthermore,

Table 3
Reliability results of the networks studied.

	Network 1	Network 2	Network 3	Network 4	Network 5	Network 6	Network 7
Demand (MW)	5700	5700	5700	5700	5700	5700	5700
EENS total (MWh/y)	75570.10	79647.85	78908.77	81611.48	81029.84	81851.03	173943.09
EENS (%)	0.151	0.160	0.158	0.163	0.162	0.164	0.348
EENS - Area A (MWh/y)	41169.40	45590.91	47585.95	55745.26	43969.82	50267.87	123024.73
EENS - Area B (MWh/y)	34175.35	34056.94	31322.82	34506.19	37060.02	31583.16	50918.36
EDNS (MW)	8.63	9.09	9.01	9.32	9.25	9.34	19.86
EFLC (outages/y)	29.93	29.85	29.15	30.23	29.66	30.27	38.7
LOLE (hours/y)	509.75	514.56	519.92	525.38	528.81	550.00	1137.01
LOLP (%)	5.82	5.87	5.94	6.00	6.04	6.28	12.98
ADLC (hours/outage)	17.03	17.24	17.84	17.38	17.83	18.17	29.38
COV EENS (%)	1.72	2.74	1.86	1.87	1.89	1.99	1.27
Computational time (hrs)	18.80	16.41	22.16	19.83	18.16	16.33	16.66

Table 4
Line loading of the interconnections.

		NTC (MW)	EE (MWh) Area A → Area B	EE (MWh) Area B → Area A	MLC (MW)	MPLC (%)	PEE (%)
Network 1	**Total exchange**	1424	57831.95	894754.01	254.58	17.88	1.90
	23-17	608	28616.16	202139.35	94.98	15.62	0.46
	13-15	608	72.76	625906.83	141.33	23.25	1.25
	07-03	208	29143.03	66707.83	91.09	43.79	0.19
Network 2	**Total exchange**	1216	126739.90	368941.09	148.58	12.22	1.00
	23-17	608	126119.28	31190.68	74.56	12.26	0.32
	13-15	608	620.62	337750.41	99.64	16.39	0.68
Network 3	**Total exchange**	816	15266.05	702066.39	205.00	25.12	1.44
	23-17	608	3697.23	508675.93	177.62	29.21	1.03
	07-03	208	11568.82	193390.46	59.99	28.84	0.41
Network 4	**Total exchange**	816	15266.05	702066.39	205.00	25.12	1.44
	13-15	608	2068.07	584605.87	169.34	27.85	1.17
	07-03	208	39782.80	85156.14	53.73	25.83	0.25
Network 5	**23-27**	608	130260.68	161135.52	145.53	23.94	0.58
Network 6	**13-15**	608	54353.14	286926.95	162.76	26.77	0.68
Network 7	**07-03**	208	188340.70	34488.39	99.62	47.89	0.45

when the cases linked by a single cross-border link (e.g., Network 5) are considered, the vulnerability worsens significantly compared to the separate case (Area A). However, by connecting the grids with two links, such as Networks 2, 3 and 4, the infrastructure's vulnerability begins to decrease because the disintegration process is slower. If a third connecting link is added, the results do not improve significantly because the structural performance never reaches the vulnerability levels of the isolated power system.

A comparison of Figs. 3(a) and (b) shows that the network with interconnections [23-17] and [13-15] provides the entire energy system better efficiency compared to the network with interconnections [23-17] and [07-03]. These empirical findings suggest that certain links provide a more robust topological structure against the propagation of cascading failures. For example, connecting two grids using links [23-17], [13-15] and [07-03] does not significantly increase the vulnerability with respect to the separate system; however, if only the case with link [07-03] is considered, the vulnerability increases dramatically compared to the case described above.

In summary, the results show that interconnections have a substantial effect on the topology because they increase the propagation of cascading events in interconnected systems. However, the number and capacity of the interconnections are relevant to minimise the impact of

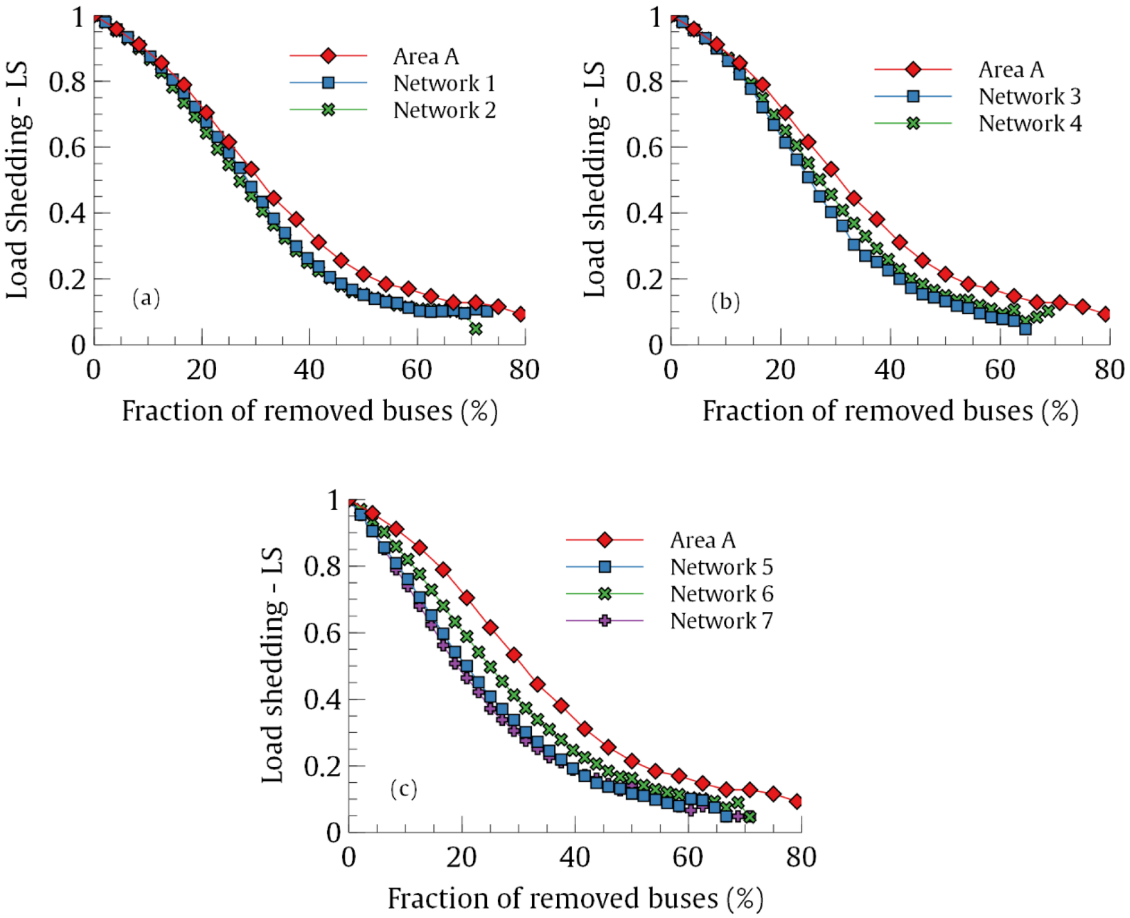

Fig. 3. Structural vulnerability results.

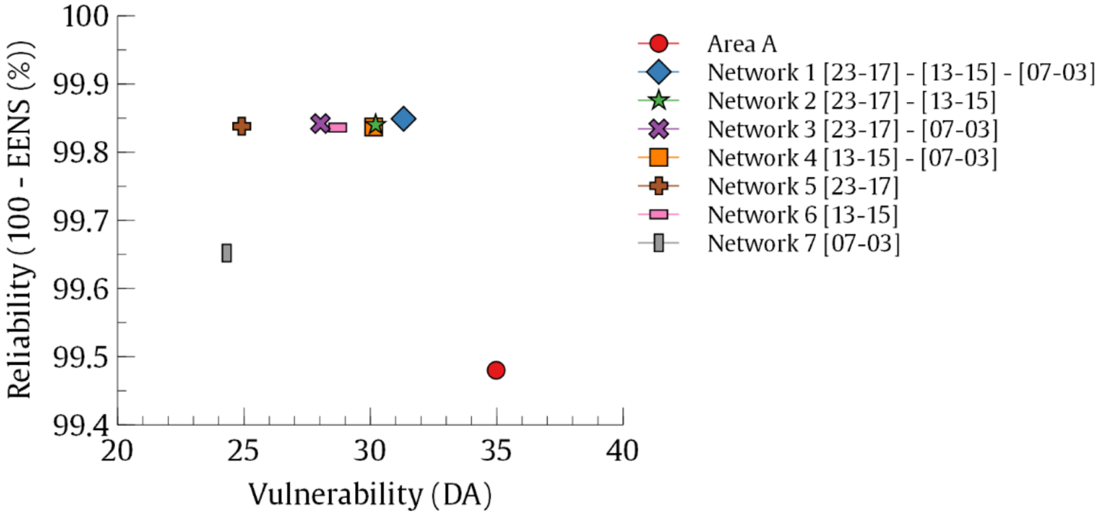

Fig. 4. Comparison between the reliability (100-EENS (%)) and vulnerability (DA) indicators.

the propagation of grid disruptions. The findings obtained here suggest similar conclusions to those shown in the papers [43] and [44].

5. Discussion of results

This study shows that reliability and vulnerability assessments are useful tools for TSOs to understand the performance and limitations of their critical infrastructure better. Therefore, this section focuses on the comparison and discussion of both approaches.

Until now, the two techniques have been used to analyse and examine different aspects of networks; however, this article considers that both approaches can be used in combination to provide a broader view of the operational performance of power systems.

The reliability results were obtained through statistical indicators that describe the operating conditions of the grid after an n-1 contingency, and the vulnerability results were plotted as decay curves that represent the topological behaviour of the studied systems against n-k contingencies. Therefore, it is proposed to determine damage areas (DAs) to accurately assess the performance of the decay curves of each result in Fig. 3. DA is defined as the region under the cascading failures curve [67]. This metric is calculated as follows:

1 Determine the equations $f(x)$ of the decay curves.
2 Calculate the integral of the equations using the fraction of removed buses as the minimum and maximum limits.

Curves near the abscissa represent greater damage to the infrastructure; thus, a small DA represents a case of severe damage, which coincides with a smaller area under the curve. Conversely, higher DA values represent less severe scenarios for the system. The use of this metric allows vulnerability indicator to be compared with reliability indicators.

Figure 4 compares the EENS (%) reliability indicators from Table 3 and the vulnerability values obtained from the plots in Fig. 3. First, the vulnerability results show that isolated systems (Area A) are more robust than interconnected grids. The isolated system (Area A) has a DA value of 35, which is significantly better than the vulnerability indicators for the other case studies corresponding to the interconnection of the two areas, which have DA values between 24 and 31. Specifically, cross-border interconnections can increase the impact of a disturbance on the vulnerability of the entire power system. Of all the cases analysed, the smallest loss of robustness is achieved in the case study of Network 1, i.e., when there is greater interconnection capacity between the two areas (through lines [23-17], [13-15] and [07-03]).

Therefore, the reliability results show that interconnected systems are more reliable than isolated systems. The information in Table 2 shows that the most interconnected case (Network 1) is less sensitive to power outages caused by a malfunction; it is more reliable. In addition, the least connected infrastructure, which is Network 7, has a higher Expected Energy Not Supplied indicator (EENS); however, this case still has better reliability than the case of the isolated grid of Area A (see EENS results in Table 1).

A joint analysis of the vulnerability and reliability indicators shown in Fig. 4 shows that Networks 1, 2, 3, 4 and 6 have small differences in both vulnerability and reliability. These cases represent a compromise solution for the design of interconnections between power systems, so the final design will only depend on the requirements of energy exchange to improve the system adequacy of the joint system (Network 1 offers an interconnection capacity of 1424 MW, Network 2 of 1216 MW, Network 3 and 4 of 816 MW, Network 6 of 608 MW). However, Networks 5 and 7 are characterised by lower robustness against cascading failures, and Network 7 (which corresponds to the interconnection of the two areas with a single low-capacity line [07-03]) has the worst reliability and the worst vulnerability of all the cases studied.

In contrast, the best results for both indicators are obtained in Network 1, which indicates that when it is necessary to connect electrical systems with cross-border lines to improve the security of supply, a greater interconnection capacity helps to improve the reliability and also provides the smallest loss of robustness in the interconnected power system.

6. Conclusions

In this article, the impacts of cross-border electricity interconnections on the reliability and vulnerability of interconnected power systems were studied. The reliability assessment was carried out by quantifying the main traditional indicators, while the vulnerability assessment was performed by considering a process of cascading failures and measuring the energy not supplied during the grid disintegration process. Both approaches were used in a comprehensive study framework that considered the fundamental specifications of their respective research fields. The simulation case studies corresponded to seven different systems obtained from the IEEE RTS-96 network.

The results showed that interconnections increase the reliability but also decrease the robustness of the entire system. This means that connection lines improve the energy exchange between the different areas that make up an interconnected infrastructure and simultaneously increase the probability that disruptions in one of the systems propagate to the others. In that case, having greater interconnection capacity is the best compromise solution for the design of transmission network topologies under reliability and robustness criteria. Thus, interconnected energy systems behave differently depending on how they are studied; however, the results obtained here could help TSOs to study the interconnection of two or more grids from a more comprehensive point of view.

CRediT authorship contribution statement

Jesus Beyza: Software, Validation, Investigation, Writing - original draft. **Pablo Gil:** Software, Validation. **Marcelo Masera:** Conceptualization, Writing - review & editing. **Jose M. Yusta:** Conceptualization, Methodology, Formal analysis, Writing - review & editing.

Acknowledgements

This study was supported by the Ministry of Economy and Competitiveness, Spain, under the project ENE2016-77172-R.

Appendix A

This appendix provides the technical data of the IEEE RTS-96 test network. The information is taken from [28]. Tables A.1–A.6

Table A.1
IEEE RTS-96 Bus Data

Bus	Bus Type	Load MW	MVAr	GL	BL	Area	Base kV	Zone
101, 201	2	108	22	0	0	11	138	11
102, 202	2	97	20	0	0	11	138	12
103, 203	1	180	37	0	0	11	138	11
104, 204	1	74	15	0	0	11	138	11
105, 205	1	71	14	0	0	11	138	11
106, 206	1	136	28	0	1.00	11	138	12
107, 207	2	125	25	0	0	11	138	12
108, 208	1	171	35	0	0	11	138	12
109, 209	1	175	36	0	0	11	138	13
110, 210	1	195	40	0	0	11	138	13
111, 211	1	0	0	0	0	11	230	13
112, 212	1	0	0	0	0	11	230	13
113, 213	3	265	54	0	0	12	230	14
114, 214	2	194	39	0	0	12	230	16
115, 215	2	317	64	0	0	12	230	16
116, 216	2	100	20	0	0	12	230	16
117, 217	1	0	0	0	0	12	230	17
118, 218	2	333	68	0	0	12	230	17
119, 219	1	181	37	0	0	12	230	15
120, 220	1	128	26	0	0	12	230	15
121, 221	2	0	0	0	0	12	230	17
122, 222	2	0	0	0	0	12	230	17
123, 223	2	0	0	0	0	12	230	15
124, 224	1	0	0	0	0	12	230	16

Note: Area A (Buses 101-124) and Area B (Buses 201-224); Bus Type: 1 (Load), 2 (Generator), 3 (Slack); GL: real component of shunt admittance; and BL: imaginary component of shunt admittance.

Table A.2
Bus load data.

Bus number	% of system load	Load MW
101, 201	3.8	108
102, 202	3.4	97
103, 203	6.3	180
104, 204	2.6	74
105, 205	2.5	71
106, 206	4.8	136
107, 207	4.4	125
108, 208	6.0	171
109, 209	6.1	175
110, 210	6.8	195
113, 213	9.3	265
114, 214	6.8	194
115, 215	11.1	317
116, 216	3.5	100
118, 218	11.7	333
119, 219	6.4	181
120, 220	4.5	128
	100	**2850**

Table A.3
Generator data

Unit group	Unit size (MW)	Unit type	Forced outage rate	MTTF (hour)	MTTR (hour)	Scheduled maintenance (weeks/year)
U12	12	Oil/Steam	0.02	2940	60	2
U20	20	Oil/CT	0.10	450	50	2
U50	50	Hydro	0.01	1980	20	2
U76	76	Coal/Steam	0.02	1960	40	3
U100	100	Oil/Steam	0.04	1200	50	3
U155	155	Coal/Steam	0.04	960	40	4
U197	197	Oil/Steam	0.05	950	50	4
U350	350	Coal/Steam	0.08	1150	100	5
U400	400	Nuclear	0.12	1100	150	6

Table A.4
Data of generators at each bus.

Bus	Unit	ID	P_g	Q_g	Q_{max}	Q_{min}	V_s
101, 201	U20	1	10	0	10	0	1.035
101, 201	U20	2	10	0	10	0	1.035
101, 201,	U76	3	76	14.1	30	-25	1.035
101, 201	U76	4	76	14.1	30	-25	1.035
102, 202	U20	1	10	0	10	0	1.035
102, 202	U20	2	10	0	10	0	1.035
102, 202	U76	3	76	7.0	30	-25	1.035
102, 202	U76	4	76	7.0	30	-25	1.035
107, 207	U100	1	80	17.2	60	0	1.025
107, 207	U100	2	80	17.2	60	0	1.025
107, 207	U100	3	80	17.2	60	0	1.025
113, 213	U197	1	95.1	40.7	80	0	1.020
113, 213	U197	2	95.1	40.7	80	0	1.020
113, 213	U197	3	95.1	40.7	80	0	1.020
114, 214	Sync Cond	1	0	13.7	200	-50	0.980
115, 215	U12	1	12	0	6	0	1.014
115, 215	U12	2	12	0	6	0	1.014
115, 215	U12	3	12	0	6	0	1.014
115, 215	U12	4	12	0	6	0	1.014
115, 215	U12	5	12	0	6	0	1.014
115, 215	U155	6	155	0.05	80	-50	1.014
116, 216	U155	1	155	25.22	80	-50	1.017
118, 218	U400	1	400	137.4	200	-50	1.050
121, 221	U400	1	400	108.2	200	-50	1.050
122, 222	U50	1	50	-4.96	16	-10	1.050
122, 222	U50	2	50	-4.96	16	-10	1.050
122, 222	U50	3	50	-4.96	16	-10	1.050
122, 222	U50	4	50	-4.96	16	-10	1.050
122, 222	U50	5	50	-4.96	16	-10	1.050
122, 222	U50	6	50	-4.96	16	-10	1.050
123, 223	U155	1	155	31.79	80	-50	1.050
123, 223	U155	2	155	31.79	80	-50	1.050
123, 223	U350	3	350	71.78	150	-25	1.050

Note: V_s is the unit's regulated voltage set-point.

Table A.5
Unit cycling restriction and ramping rates

Unit group	Unit size (MW)	Unit type	Min. downtime (hours)	Min. uptime (hours)	Ramp rate (MW/ minute)
U12	12	Oil/Steam	2	4	1
U20	20	Oil/CT	1	1	3
U50	50	Hydro	N/A		
U76	76	Coal/Steam	4	8	2
U100	100	Oil/Steam	8	8	7
U155	155	Coal/Steam	8	8	3
U197	197	Oil/Steam	10	12	3
U350	350	Coal/Steam	48	24	4
U400	400	Nuclear	1	1	20

Table A.6
Data of branches

ID	From	To	L	λ_p	Dur.	λ_t	R	X	B	Con.	LTE	STE	Tr.
A1	101	102	3	0.24	16	0.0	0.003	0.014	0.461	175	193	200	0
A2	101	103	55	0.51	10	2.9	0.055	0.211	0.057	175	208	220	0
A3	101	105	22	0.33	10	1.2	0.022	0.085	0.023	175	208	220	0
A4	102	104	33	0.39	10	1.7	0.033	0.127	0.034	175	208	220	0
A5	102	106	50	0.48	10	2.6	0.050	0.192	0.052	175	208	220	0
A6	103	109	31	0.38	10	1.6	0.031	0.119	0.032	175	208	220	0
A7	103	124	0	0.02	768	0.0	0.002	0.084	0.000	400	510	600	1.015
A8	104	109	27	0.36	10	1.4	0.027	0.104	0.028	175	208	220	0
A9	105	110	23	0.34	10	1.2	0.023	0.088	0.024	175	208	220	0
A10	106	110	16	0.33	35	0.0	0.014	0.061	2.459	175	193	200	0
A11	107	108	16	0.30	10	0.8	0.016	0.061	0.017	175	208	220	0
AB1	107	203	42	0.44	10	2.2	0.042	0.161	0.044	175	208	220	0
A12-1	108	109	43	0.44	10	2.3	0.043	0.165	0.045	175	208	220	0
A13-2	108	110	43	0.44	10	2.3	0.043	0.165	0.045	175	208	220	0
A14	109	111	0	0.02	768	0.0	0.002	0.084	0.000	400	510	600	1.030
A15	109	112	0	0.02	768	0.0	0.002	0.084	0.000	400	510	600	1.030
A16	110	111	0	0.02	768	0.0	0.002	0.084	0.000	400	510	600	1.015
A17	110	112	0	0.02	768	0.0	0.002	0.084	0.000	400	510	600	1.015
A18	111	113	33	0.40	11	0.8	0.006	0.048	0.100	500	600	625	0
A19	111	114	29	0.39	11	0.7	0.005	0.042	0.088	500	600	625	0
A20	112	113	33	0.40	11	0.8	0.006	0.048	0.100	500	600	625	0
A21	112	123	67	0.52	11	1.6	0.012	0.097	0.203	500	600	625	0
A22	113	123	60	0.49	11	1.5	0.011	0.087	0.182	500	600	625	0
AB2	113	215	52	0.47	11	1.3	0.010	0.075	0.158	500	600	625	0
A23	114	116	27	0.38	11	0.7	0.005	0.059	0.082	500	600	625	0
A24	115	116	12	0.33	11	0.3	0.002	0.017	0.036	500	600	625	0
A25-1	115	121	34	0.41	11	0.8	0.006	0.049	0.103	500	600	625	0
A25-2	115	121	34	0.41	11	0.8	0.006	0.049	0.103	500	600	625	0
A26	115	124	36	0.41	11	0.9	0.007	0.052	0.109	500	600	625	0
A27	116	117	18	0.35	11	0.4	0.003	0.026	0.055	500	600	625	0
A28	116	119	16	0.34	11	0.4	0.003	0.023	0.049	500	600	625	0
A29	117	118	10	0.32	11	0.2	0.002	0.014	0.030	500	600	625	0
A30	117	122	73	0.54	11	1.8	0.014	0.105	0.221	500	600	625	0
A31-1	118	121	18	0.35	11	0.4	0.003	0.026	0.055	500	600	625	0
A31-2	118	121	18	0.35	11	0.4	0.003	0.026	0.055	500	600	625	0
A32-1	119	120	27.5	0.38	11	0.7	0.005	0.040	0.083	500	600	625	0
A32-2	119	120	27.5	0.38	11	0.7	0.005	0.040	0.083	500	600	625	0
A33-1	120	123	15	0.34	11	0.4	0.003	0.022	0.046	500	600	625	0
A33-2	120	123	15	0.34	11	0.4	0.003	0.022	0.046	500	600	625	0
A34	121	122	47	0.45	11	1.2	0.009	0.068	0.142	500	600	625	0
AB3	123	217	51	0.46	11	1.3	0.010	0.074	0.155	500	600	625	0

Note: ID (Branch identifier. Inter area branches are indicated by double letter ID); λ_p (Permanent outage rate [outage/year]); Dur. (Permanent outage duration [hrs]); λ_t (Transient outage rate [outages/year]); Con. (Continuous rating); LTE (Long-time emergency rating [24 hrs]); STE (Short-time emergency rating [15 min]); Tr. (Transformer off-nominal ratio).

Algorithm 1
. Quantification of the effect of interconnections on the vulnerability of power grids.

```
Input: Information about the power grid and $\Delta$.
Output: LS.
Step 1: Initialization: $n=1$, $LS=1$, $N = N_{Buses}$; set the sample threshold $\Delta$;
Step 2: Power flows calculation: use DCOPF to calculate the load flows in the system;
    calculate $\sum_i P_{Di}^{BC}$ for the base case;
Step 3: Starting point: randomly select a bus of the system as the first node to be
    eliminated ($N_{eliminated} \neq B_{slack}$);
Step 4: New topology: eliminate all links adjacent to the node removed in Step 3;
    determine the number of islands and identify the island that contains the slack
    generator;
Step 5: Power flows calculation: run DCOPF on the network from Step 4;
Step 6: LS calculation: use equation (9) and calculate the $LS^n_{N_{eliminated}}(x)$ of the grid
    that corresponds to node $N_{eliminated}$ of sample $n$ at the $x$-th contingency;
Step 7: New node selection: randomly eliminate a new node from the network from
    Step 4 if $\Sigma N_{eliminated} < N$ and go to Step 4; otherwise, go to Step 8;
Step 8: Set $n = n + 1$;
Step 8: Ending: if $n > \Delta$, the algorithm ends; otherwise, go to Step 1;
Step 9: Results: Average the $LS$ results of all $\Delta$ samples.
```

References

[1] E. Commission, “Electricity interconnection targets,” 2019. [Online]. Available:https://ec.europa.eu/energy/en/topics/infrastructure/projects-common-interest/electricity-interconnection-targets.

[2] Report of the Commission Expert Group on electricity interconnection targets, “Towards a sustainable and integrated Europe Report of the Commission Expert Group on electricity interconnection targets,” 2017.

[3] Svendsen HG, Spro OC. PowerGAMA: A new simplified modelling approach for analyses of large interconnected power systems, applied to a 2030 Western Mediterranean case study. J. Renew. Sustain. Energy 2016;8(5).

[4] ENTSOE, “Final Report System Disturbance on 4November 2006,” Nov-. [Online]. Available:https://www.entsoe.eu/fileadmin/user_upload/_library/publications/ce/otherreports/Final-Report-20070130.pdf.

[5] Ouyang M, Pan Z, Hong L, Zhao L. Correlation analysis of different vulnerability metrics on power grids. Phys. A Stat. Mech. its Appl. 2014;396:204–11.

[6] Gupta S, Kazi F, Wagh S, Singh N. Analysis and prediction of vulnerability in smart power transmission system: A geometrical approach. Int. J. Electr. Power Energy Syst. 2018;94:77–87.

[7] Ali Kadhem A, Abdul Wahab NI, Aris I, Jasni J, Abdalla AN. Computational techniques for assessing the reliability and sustainability of electrical power systems: A review. Renew. Sustain. Energy Rev. 2017;80:1175–86.

[8] Clausen J, Hansson SO, Nilsson F. Generalizing the safety factor approach. Reliab. Eng. Syst. Saf. 2006;91(8):964–73.

[9] Billinton R, Sankarakrishnan A. Comparison of Monte Carlo simulation techniques for composite power system reliability assessment. IEEE WESCANEX Commun. Power, Comput. 1995;1(95):145–50.

[10] Zio E. An Introduction to the Basics of Reliability and Risk Analysis 13. World Scientific Publishing Company; 2007.

[11] Rausand M, Høyland A. System reliability theory : models, statistical methods, and applications. Wiley-Interscience; 2004.

[12] Aven T. Foundations of Risk Analysis. Wiley; 2003.

[13] Allan R, Billinton R. Probabilistic assessment of power systems. Proc. IEEE 2000;88(2):140–62.

[14] T. H. Murray, Alan T; Grubesic, “Critical Infrastructure: Reliability and Vulnerability,” Springer. pp. 1–8, 2007.

[15] Johansson J, Hassel H, Zio E. Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems. Reliab. Eng. Syst. Saf. 2013;120:27–38.

[16] Apostolakis GE. How Useful Is Quantitative Risk Assessment? Risk Anal 2004;24(3):515–20.

[17] Aven T. A semi-quantitative approach to risk analysis, as an alternative to QRAs. Reliab. Eng. Syst. Saf. 2008;93(6):790–7.

[18] Aven T, Renn O. The role of quantitative risk assessments for characterizing risk and uncertainty and delineating appropriate risk management options, with special emphasis on terrorism risk. Risk Analysis 2009;29(4):587–600.

[19] Zio E. Reliability engineering: Old problems and new challenges. Reliability Engineering and System Safety 2009;94(2):125–41.

[20] Abedi A, Beyza J, Romerio F, Dominguez-Navarro JA, Yusta JM. MCDM approach for the integrated assessment of vulnerability and reliability of power systems. IET Gener. Transm. Distrib. 2019;13(20):4741–6.

[21] McEntire DA. Why vulnerability matters: Exploring the merit of an inclusive disaster reduction concept. Disaster Prev. Manag. An Int. J. 2005;14(2):206–22.

[22] Haimes YY. On the definition of vulnerabilities in measuring risks to infrastructures. Risk Anal 2006;26(2):293–6.

[23] Cuadra L, Salcedo-Sanz S, Del Ser J, Jiménez-Fernández S, Geem ZW. A critical review of robustness in power grids using complex networks concepts. Energies 2015;8(9):9211–65.

[24] Veloza OP, Santamaria F. Analysis of major blackouts from 2003 to 2015: Classification of incidents and review of main causes. Electr. J. 2016;29(7):42–9.

[25] Johansson J, Hassel H, Zio E. Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems. Reliab. Eng. Syst. Saf. 2013;120:27–38.

[26] Alipour Z, Monfared MAS, Zio E. Comparing topological and reliability-based vulnerability analysis of Iran power transmission network. Proc. Inst. Mech. Eng. Part O J. Risk Reliab. 2014;228(2):139–51.

[27] Blockley DI, Agarwal J, Pinto JT, Woodman NJ. Structural vulnerability, reliability and risk. Prog. Struct. Eng. Mater. 2002;4(2):203–12.

[28] Task Reliability Test System. The IEEE reliability test system -1996 a report prepared by the reliability test system task force of the application of probability methods subcommittee. IEEE Trans. Power Syst. 1999;14(3):1010–20.

[29] Energy Exemplar, “PLEXOS® Simulation Software,” 2019. [Online]. Available: https://energyexemplar.com/products/plexos-simulation-software/.

[30] Energy Systems Modelling Project, “PLEXOS,” 2019. [Online]. Available: http://www.reeem.org/index.php/plexos/.

[31] Beyza J, Yusta M J, Correa J G, Ruiz F H. Vulnerability Assessment of a Large Electrical Grid by New Graph Theory Approach. IEEE Lat. Am. Trans. 2018;16(2):527–35.

[32] Wangdee W. Bulk electric system reliability simulation and application. Univ. Saskatchewan 2005:1–290.

[33] Billinton R, Li W. Reliability Assessment of Electric Power Systems Using Monte Carlo Methods. Boston, MA: Springer US; 1994.

[34] Billinton R, Allan RN. Reliability Evaluation of Power Systems 53. Boston, MA: Springer US; 1996.

[35] Wolf S. Clarifying vulnerability definitions and assessments using formalisation. Int. J. Clim. Chang. Strateg. Manag. 2013;5(1):1756–8692.

[36] Abedi A, Gaudard L, Romerio F. Review of major approaches to analyze vulnerability in power system. Reliability Engineering and System Safety 183. Elsevier Ltd; 2019. p. 153–72.

[37] Kröger W, Zio E. Vulnerable Systems. London: Springer London; 2011.

[38] Milanovic JV, Zhu W. Modeling of interconnected critical infrastructure systems using complex network theory. IEEE Trans. Smart Grid 2018;9(5):4637–48.

[39] Zio E. Challenges in the vulnerability and risk analysis of critical infrastructures. Reliab. Eng. Syst. Saf. 2016;152:137–50.

[40] E. Zio Politecnico di Milano, G. Sansavini ETH Zurich, E. Zio, R. Piccinelli, and G. Sansavini, “An All-Hazard Approach for the Vulnerabil-ity Analysis of Critical Infrastructures,” pp. 2451–2458, 2011.

[41] Holmgren ÅJ. Using graph models to analyze the vulnerability of electric power networks. Risk Anal 2006;26(4):955–69.

[42] Bompard E, Napoli R, Xue F. Vulnerability of interconnected power systems to malicious attacks under limited information. Eur. Trans. Electr. Power 2008;18(8):820–34.

[43] Zhang W, Xia Y, Ouyang B, Jiang L. Effect of network size on robustness of interconnected networks under targeted attack. Phys. A Stat. Mech. its Appl. 2015;435:80–8.

[44] Xia Y, Zhang W, Zhang X. The effect of capacity redundancy disparity on the robustness of interconnected networks. Phys. A Stat. Mech. its Appl. 2016;447:561–8.

[45] Brummitt CD, D'Souza RM, Leicht EA. Suppressing cascades of load in interdependent networks. Proc. Natl. Acad. Sci. 2012;109(12):E680–9.

[46] Tan F, Xia Y, Zhang W, Jin X. Cascading failures of loads in interconnected networks under intentional attack. Epl 2013;102(2).

[47] C.-W. Ten, K. Yamashita, Z. Yang, A. V. Vasilakos, and A. Ginter, “Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems,” vol. 3053, no. c, pp. 1–21, 2018.

[48] Che L, Liu X, Ding T, Li Z. Revealing Impacts of Cyber Attacks on Power Grids Vulnerability to Cascading Failures. IEEE Trans. Circuits Syst. II Express Briefs 2018;PP,(c). 1–1.

[49] Bompard E, Estebsari A, Huang T, Fulli G. A framework for analyzing cascading failure in large interconnected power systems: A post-contingency evolution simulator. Int. J. Electr. Power Energy Syst. 2016;81:12–21.

[50] Bompard E, Pons E, Wu D. Analysis of the structural vulnerability of the interconnected power grid of continental Europe with the Integrated Power System and Unified Power System based on extended topological approach. Int. Trans. Electr. Energy Syst. 2013;23(5):620–37.

[51] Siami M, Motee N. Fundamental limits on robustness measures in networks of interconnected systems. Proc. IEEE Conf. Decis. Control 2013:67–72.

[52] Milanovic JV, Zhu W. Modelling of Interconnected Critical Infrastructure Systems Using Complex Network Theory. IEEE Trans. Smart Grid 2017;3053(c):1.

[53] Mladjao MAM, Ikram EA, Abdel-Moumen D, Mohammed EG. New Robust Energy Management Model for Interconnected Power Networks Using Petri Nets Approach. Smart Grid Renew. Energy 2016;07(01):46–65.

[54] ENTSOE, “P3 – Policy 3: Operational Security.” 2009.

[55] Billinton R, Jonnavithula A. Application of sequential Monte Carlo simulation to evaluation of distributions of composite system indices. IEE Proc. Gener. Transm. Distrib. 1997;144(2):87–90.

[56] Wangdee W, Billinton R. Reliability performance index probability distribution analysis of bulk electricity systems. Canadian Conference on Electrical and Computer Engineering. 2005. 2005. p. 445–9.

[57] Ahern EP, Deane P, Persson T, Ó Gallachóir B, Murphy JD. A perspective on the potential role of renewable gas in a smart energy island system. Renew. Energy 2015;78:648–56.

[58] C. Meyers, F. Streitz, Y. Yao, S. Smith, and A. Lamont, “Using Supercomputers to Speed Execution of the CAISO/PLEXOS 33% RPS Study,” 2007.

[59] R. Johnson, “Reliability Analysis using PLEXOS.” [Online]:https://energyexemplar.com/wp-content/uploads/Reliability-Analysis-Using-PLEXOS.pdf.

[60] Bier VM, Gratz ER, Haphuriwat NJ, Magua W, Wierzbicki KR. Methodology for identifying near-optimal interdiction strategies for a power transmission system. Reliab. Eng. Syst. Saf. 2007;92(9):1155–61.

[61] Haidar AM, Mohamed A, Hussain A. Vulnerability assessment of a large sized power system considering a new index based on power system loss. Eur. J. Sci. Res. Eur. J. Sci. Res. J. Electr. Eng. Technol. 2007;17(2):61–72.

[62] Zhu Y, Yan J, Tang Y, Sun Y, He H. Resilience analysis of power grids under the sequential attack. IEEE Trans. Inf. Forensics Secur. 2014;9(12):2340–54.

[63] Ouyang M. Comparisons of purely topological model, betweenness based model and direct current power flow model to analyze power grid vulnerability. Chaos 2013;23(2).

[64] 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.

[65] Anderson DR, Sweeney DJ, Williams TA. Essentials of statistics for business and economics. 2011. South-Western.

[66] S. Even, “Depth-First Search,” Graph Algorithms, pp. 46–64.

[67] Beyza J, Garcia-Paricio E, Yusta JM. Ranking critical assets in interdependent energy transmission networks. Electr. Power Syst. Res. 2019;172:242–52.