Reliability Engineering and System Safety 183 (2019) 153–172

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Review of major approaches to analyze vulnerability in power system

Amin Abedi[a,*], Ludovic Gaudard[b], Franco Romerio[a,c]

[a] Institute for Environmental Sciences, University of Geneva, Switzerland
[b] Precourt Energy Efficiency Center, Management Science and Engineering, Stanford University, USA
[c] Geneva School of Economics and Management, University of Geneva, Switzerland

ARTICLE INFO

Keywords:
Vulnerability analysis
Critical infrastructure
Power grid
Blackout

ABSTRACT

The failure of a power system as a critical infrastructure causes considerable damage to society. Hence, the vulnerabilities of such facilities should be minimized to cope with several sources of disruption. Various methods have been proposed to identify and address the weaknesses of power systems to enhance their robustness and resilience. As the field is evolving quickly, understanding the pros and cons of each approach and the trends could be challenging. This paper aims to guide the reader toward choosing the most effective method according to the issue investigated. We focus on studies on power grids; however, research on other critical infrastructure could also benefit from this review.

We identified three classes of events, namely natural hazards, intentional attacks, and random failures. These events affect the adopted method that can range from analytical approaches—complex network, flow-based, logical, and functional methods—to Monte Carlo simulations. At present, hybrid approaches are emerging with the growing complexities of power grids. Various methods are used in combination to benefit from the strengths of one another. We identified three emerging topics and challenges that require further investigations, namely the N-k problem, trade-off between robustness and optimality, and emerging drivers in power grids.

1. Introduction

An electric system represents a "critical infrastructure" (CI) [1]. Any failure or destruction affects the safety, security, economy, health, and well-being of a community [2]. According to a recent report [3], increasing energy consumption exceeds the slow deployment of energy infrastructure in many countries. An ill-designed electricity reform can even worsen the problem [4]. Deregulation, the opening of the market to competition, and decarbonization may represent a challenge for an electric system [5]. The operators must deal with capacity and design limitations [6, 7] to avoid perturbation.

The risk of blackouts must be handled, and this includes managing the cascading effect. It happens when a triggering event, e.g. the disruption of a transmission line, leads to the overload of the remaining lines and disconnects them from the network [8, 9]. Even in a network with a low probability of occurrence of a blackout, the risk remains high as the impact of an event involves substantial social and economic costs. Power failures have recently affected hundreds of millions of people. In 2003, three independent events in Iran, North America, and Italy hit a total of 128 million people. In 2012 and 2015, 670 million Indian people and 70 million Turkish people respectively were temporarily deprived of power [10-13]. In the USA, the annual cost of weather-related blackouts ranges from $20–$55 billion. The frequency has even increased over the last 30 years [14, 15]. In Switzerland, 24 hours without electricity costs about $2–4 billion, exceeding the daily GDP [16, 17].

Deploying robust and resilient CI can limit this risk. Operators must detect and rank the most vulnerable elements of a system under a variety of attack scenarios [18]. They can therefore design and control systems to reduce their vulnerability to unpredictable events [19]. Scientists have been developing innovative methods to support decision-makers in this task. However, grasping the pros and cons of such methods is becoming challenging, as the field evolves quickly.

Three contributions have already reviewed the field, but they have focused on complex network (CN) concepts [20-22]. Cuadra et al. [20] considered both pure and extended CN approaches; Bompard et al. [21] focused on their own previous research works, while Pagani and Aiello [22] reviewed literature from a statistic perspective. In 2015, reviews on a specific approach were relevant and insightful. However, the field has considerably expanded since. Besides a required update, an overview of a larger spectrum of methods is becoming critical. New investigations tend to favor hybrid approaches; scholars must understand the pros and cons of each method to merge the complementary ones.

In this paper, we review the most recent scientific studies on the vulnerability of power grids. It introduces CN but also considers power flow, logical, and functional methods. We compare and categorize them

* Corresponding author.

https://doi.org/10.1016/j.ress.2018.11.019
Received 14 March 2018; Received in revised form 10 November 2018; Accepted 21 November 2018
Available online 22 November 2018
0951-8320/

according to several criteria, including the methodology used, assumptions, test cases, failure scenarios, and modeling capability (node and/or line modeling). To further contrast the methods, we provide a correlation analysis of results, and, finally, highlights the emerging challenges.

The rest of this paper is organized as follows. Section 2 provides some basic definitions. Section 3 introduces different methods of vulnerability analysis. We compare the methods in Section 4 and underline some emerging topics and challenges in this field. Finally, Section 5 summarizes the main findings and presents the conclusions.

2. Definitions

2.1. Critical infrastructure

Infrastructure is large-scale man-made systems that operate interdependently to provide and deliver essential goods and services [1, 23]. They are considered critical if their failure or destruction has a considerable impact on the safety, security, economy, health, and well-being of a community. Typical examples are energy and communication networks, transportation systems, and water and gas distribution systems [1, 24, 25].

Interdependency among CIs leads to the concept of "systems-of-systems" (SOS) [26]. While interdependencies can improve the CIs' operational efficiency, they also increase their vulnerability [27]. In this perspective, assessing the mutual interdependency of CIs to develop adequate protection is necessary [28]. A range of literature [29-38] introduces four types of interdependencies: physical, cyber, geographic, and logical.

2.2. Cascading outage and blackout

"Cascading outage" starts from a specific event that leads to a sequence of disconnections and failures. It turns into a "blackout" when it affects a wide area [20]. According to [39], the probability of a blackout decreases with its size. Doubling the blackout size (power, energy, or the number of failures) halves its probability, which approximately follows a -1 to -2 power law [40-42]. However, Prieto et al. [43] suggest that the probability rather obeys a Pareto II distribution, i.e. a shifted power law distribution. Thus, despite a low probability of blackouts, the likelihood of large blackouts seems higher than expected [42, 44].

Even with a low probability, the risk of blackouts is still high. Indeed, the risk assessment also considers the size of the impact, which could be large, as shown in Table 1. Some studies also [44-49] provide lessons to be learned from historical events.

2.3. Power system hazards

CIs are usually subject to many types of hazards and events [1, 52]. Based on the literature review, Fig. 1 suggests a consistent taxonomy that differentiates random failures, natural hazards, and intentional attacks (pointwise and regional attacks). It represents a finer categorization than the one suggested by Murray and Grubesic [53], who distinguished accidental events from deliberate ones. We further describe and justify the three suggested categories in the coming subsections.

2.3.1. Random failures

Random failures affect all similar components of an infrastructure with the same probability distribution. The position of a specific node in the network has no impact on the probability of failure. The literature usually considers the following random disruptions:

- Power system component failures due to component aging, communication system failures, an IT fault, etc. [54],
- Hidden failures that play an important role in cascading events due to an incorrect removal of the power system components by a protection system [55, 56],
- Sabotages, as far as terrorists or enemies do not possess any information about the power grid [57] (see Section 2.3.3 in the case when they possess this information),
- Imbalances between load and generation [20],
- Human errors [58].

The impact of such an event is usually investigated by randomly removing a number of CI components [27]. The system behavior without these elements highlights its vulnerability and robustness. Other studies also consider vulnerability due to the imbalance between load and generation. They alter the loads or power generation in some randomly selected nodes and observe the system reaction [59].

2.3.2. Natural hazards

Natural phenomena, e.g. earthquakes, hurricanes, and lightning, can also alter CIs [15]. Contrary to random failures, the geographic position affects the probability of disruption of a component. Natural events can directly destruct CIs' elements, such as high winds or landslides that damage electric towers. They also indirectly perturb the system. For instance, cold waves and ice can reduce the distance between conductors up to that of generating flash [14]. Heat waves can lower the capacity of an electric line up to the point of overloading it. In Europe, four nuclear power plants had to be shut down in 2003 due to the increase in the temperature of rivers, water from which is used for cooling the reactor cores. Such events affected 4 GW of the power supply, leading to approximately $14.5 billion financial losses [60].

Natural hazards represent a significant cause of power system disruptions. Adverse weather conditions caused approximately 33% of the outages in Canada over a 20-year period [61]. Meteorological events caused 43% of 400-kV and 48% of 154-kV line failures in Turkey over a 2-year period [3]. These events usually impose relatively long-duration interruptions, ranging from hours to days, resulting in heavy losses. In the USA, weather-related blackouts cost about $20 to 55 billion per year [14].

2.3.3. Intentional attacks

An effective intentional attack targets the critical elements of the

Table 1
Some recent large-scale blackouts in the world and their consequences.

No.	Country	Year	Load loss (GW)	Economic loss	People affected (*Million)	Duration (hours)	Reference
1	Iran	2003	~7	Not available	22	8	[10, 13]
2	USA, Canada	2003	61.8	$ 6.4 billion	50	16–72 (USA), up to 192 (Canada)	[10-12]
3	Italy	2003	24	Over €120 million	~56	Up to ~18	[10, 12]
4	Russia	2005	~3.5	$ 1–2 billion	4	~4	[46, 50]
5	Western Europe	2006	~14	Not available	15	~2	[12]
6	USA and Mexico	2011	4.3	Up to $118 million	Over 5	~11	[50]
7	India	2012	~48	Not available	670	2–8	[13, 51]
8	Turkey	2015	32.2	Not available	70	More than 7	[13]

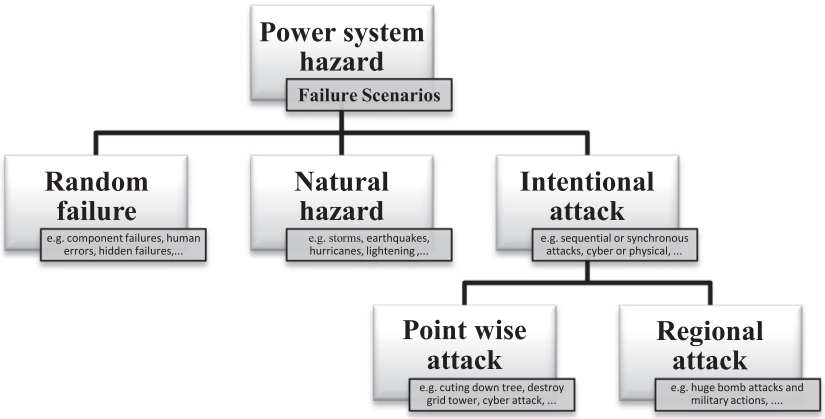

Fig. 1. Different failure scenarios in power systems.

Table 2
Different vulnerability definitions.

Group	No.	Definition	Reference (Page number)
Physical vulnerability	1	"A physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard."	[79] (2)
	2	"The weakness level of a system to failures, disasters, or attacks."	[23] (1)
	3	"A susceptibility (sensitivity) to threats and hazards that substantially reduce the ability of a system to maintain its intended function."	[53, 80] (39,23)
	4	"A physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard."	[79] (2)
Systemic vulnerability	5	"The manifestation of the inherent states of the system (e.g., physical, technical, organizational, cultural) that can be exploited to adversely affect (cause harm or damage to) that system."	[81] (1)
	6	"The conditions determined by physical, social, economic and environmental factors or processes, which increase the susceptibility of a community to the impact of hazards."	[82] (13)
	7	"The inability of a system to withstand strains and the effects of failures."	[83] (2)
Systemic and physical	8	"Any weakness in an asset's or infrastructure's design, implementation, or operation that can be exploited by an adversary."	[25] (10)
Measure	9	"A measure of the system's weakness with respect to a sequence of cascading events that may include line or generator outages, malfunctions or undesirable operations of protection relays, information or communication system failures, and human errors."	[84] (1)
	10	"Robustness or vulnerability (its opposite concept) are often used to measure to what extent a power grid has high or low reliability, respectively."	[20] (2)
	11	"The performance drop of a power grid under a disruptive event."	[85] (2)

CIs. Therefore, the probability of failure and randomness are not at stake. Power grids are attractive for intentional attacks, as they suffer from the following inherent characteristics [7]:

- Components of power grids are usually distributed in some wide geographical areas,
- Critical elements are spatially concentrated (e.g., substations) and vulnerable to common-cause initiating events,
- Most of the components are not guarded,
- Most of the critical components are located outdoor and thus particularly vulnerable to several threats,
- The impact of a blackout may be significant for a society.

The intentional attacks might be cyber or physical. Physical damage can be as simple as cutting down trees or tripping transmission lines. An individual physically destroyed a local high-voltage transmission line in Arkansas, which resulted in 10,000 customers suffering without electric power on October 6, 2013 [62]. Sudden bursts of electromagnetic radiation (electromagnetic pulse) can also be generated to destabilize the power grid [63]. According to [64], successful or failed attacks targeted 528 substations and 2,539 transmission towers in the world between 1996 and 2006.

In contrast, cyber attackers inject false data to mislead the system operator. If they know the entire power grid topology and attributes, they can fulfill the physical laws (e.g. power flow laws) without being detected by the system operator [65, 66]. They can also send false topology information to control centers. For instance, they can indicate a tripped line as a connected one and vice versa [66, 67]. Attacks can also rely on partial information. False data can target smart meters in a specific area that require only local information. Then, the disruption can spread to the rest of the network without being detected by the system operator [68, 69].

Intentional attacks can be divided into pointwise (nonproximity-based) and regional (proximity-based) [27, 70, 71]. Pointwise attack scenarios ignore the geographical location of the components. The attacker optimizes the impact by considering the centrality of each node or edge, as defined in Section 3. The regional attacks select a set of local nodes, edges, or paths [72] to sabotage, e.g., with bombs and weapons [27].

2.4. Vulnerability

Despite vulnerability being a common concept, Wolf et al. [73] observed more than 20 definitions of vulnerability. Various disciplines have been considering this concept, resulting in its diverse definitions and making consensus difficult. Vulnerability can be social, organizational, economic, environmental, territorial, physical, and systemic [74, 75]. As the literature we reviewed is more specific, we can identify

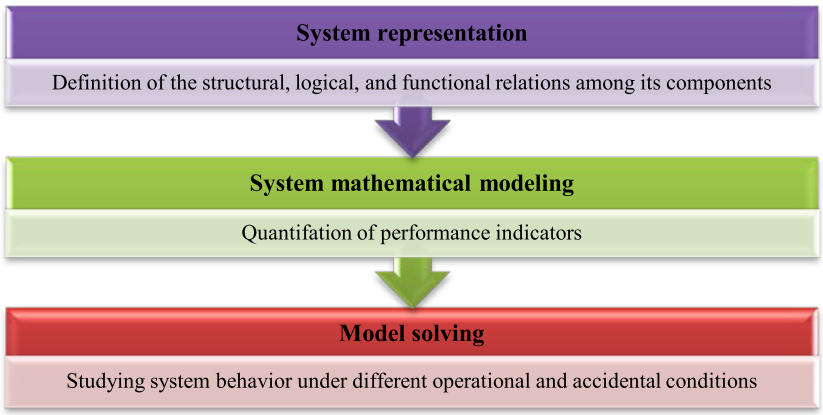

Fig. 2. Main steps of vulnerability analysis.

some trends. Table 2 provides the list of definitions we found during our review process. Most studies focus on physical and systemic vulnerability.

Physical vulnerability represents the degree of loss of an element due to external pressure such as natural hazards [76]. It mainly focuses on the features and assets that can lead the whole system to fail, as in definitions 1 to 4. In contrast, definitions 5 to 7 are related to systemic vulnerability. They consider the degree of redundancy, functionality, and dependency of a system due to the failure of a specific element or interconnected system [77]. Therefore, understanding the conditions or states that can lead the system to fail is crucial. Some papers, especially in the field of natural hazards, integrate both physical element failures (physical vulnerability) and system functionality (systemic vulnerability) [24, 78], as seen in definition 8. Finally, we added a third group of definitions that focus on the measure of the system weakness to hazards: definitions 9–11.

3. Approaches to vulnerability analyses

Vulnerability analysis usually includes the different steps shown in Fig. 2 [19]. It aims to [1, 28, 53, 86, 87]:

- Determine the critical components that require protection (according to their location, function, or carried load [88]),
- Identify possible undesirable events and their impacts,
- Prioritize the components based on the consequence of loss, e.g., the rate of important blackouts (number per year) and their severity, e.g. power lost and not supplied energy [83],
- Identify potential and inherent vulnerabilities,
- Identify existing countermeasures and their level of effectiveness [89, 90],
- Estimate the degree of vulnerability relative to each component.

Vulnerability analysis can be carried out within two different scenarios: static and dynamic [91-93]. In the static analysis of robustness, one removes a node from a network without any redistribution of its loads (or flows). In the dynamic analysis, flows are redistributed in the network after a node or link failure. This approach is more complicated and may need to be solved numerically [91-93].

Scientists have been developing various methods to assess the vulnerability of CIs. The approach to be adopted depends on the relevant issue and the type of hazards investigated. This paper guides the reader in the choice of the right/relevant method. Fig. 3 provides a first overview.

Vulnerability analysis is performed either by using analytical techniques or by simulation [14, 83]. The main conceptual differences are as follows [83, 94-96]:

- Analytical techniques give an exact solution to a simplified problem, whereas simulations provide an accurate solution to an exact problem,
- Analytical techniques are quicker for the assessment of several similar systems. It performs well at solving a problem for a given set of parameters. In contrast, building a simulation model can consume less time than deriving the equations,
- Analytical techniques evaluate the indices of a simplified model using mathematical solutions. Monte Carlo simulation methods [97] estimate the indices by simulating the actual process and the random behavior of the system,
- With increasing complexity, formulae become more challenging to derive. The last resort is often simulation,
- Analytical approaches use mathematical equations and models, e.g. block diagrams or fault trees, to derive related indices. These approaches require approximations and simplifications when analyzing complex systems.

The forthcoming section will follow the structure of Fig. 3. We introduce each method one by one. However, we omitted to develop Monte Carlo simulations to avoid making this paper excessively long. The above-presented differences with analytical approaches already provide a good overview.

The four following sections, each ending with a table, categorize the reviewed papers according to three aspects of information (metric/indicator; case study dimensions; assumptions, and failure scenarios). We collected these data because they affect each other. In particular, despite no fixed rules existing, the size of a case study tends to determine the suitable assumptions. Studies are presented in a chronological order in the tables to provide a good understanding of the evolution in this field of research. These tables also save time and help a researcher efficiently select the studies that are relevant for a specific research topic.

3.1. Topological method (complex network analysis)

Complex network analysis (CNA) has been developed recently [98]. The first systematic studies appeared in the late 1990 s to study and analyze the structure, dynamics, and evolution of many complex systems [22, 99]. CNA is performed not only in power grids but also in several other human-made systems, including railway networks, public transportation networks, road and rail transportation, airports, process plants, the Internet, the topology of web pages, airline routes, and electronic circuits [87, 100-108]. It has also been applied to socio-economic systems, e.g. communication and social networks [109-112]. This method also works for systems stemming from nature, e.g. evolution, metabolic networks, protein interactions, biology, and food webs [20, 113, 114].

CNA considers a set of nodes or vertices, e.g. substations or power

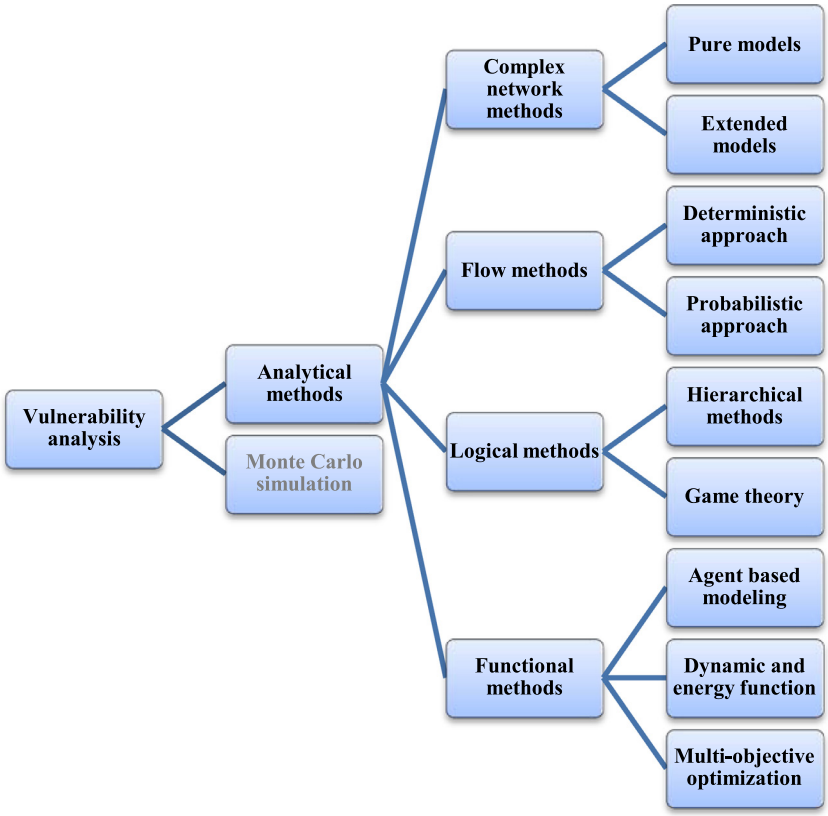

Fig. 3. Different Methods for Vulnerability Analysis.

plants, interconnected by means of links or edges, e.g. power transmission lines [20]. Some metrics and indices, namely centralities, identify the most critical nodes and edges [8, 107]. According to this concept of centrality, an individual closer to many people will obtain more critical information. This opportunity increases his/her power and influence [115].

CNA is segmented into two broad approaches. Pure models focus on topological definitions, such as degree, closeness, betweenness, clustering coefficient, and efficiency. In the second approach, extended models add electrical elements into the CNA. For instance, they account for the electrical and reliability features of power grids, e.g. impedance, power, and capacitance of the components. This approach triggered the development of extended centralities, such as electrical betweenness and net-ability [20, 116].

Some papers also distinguish weighted/unweighted and directed/undirected models. Weights allow considering the properties of a component, e.g. its cost, reliability, capacities, power, and impedance [91, 117]. Directions are applied to edges to include the actual constraint of flows or goods between nodes. For instance, power always flows from generators to loads [20]. While [118-124] provide extended information about CNA, the two following subsections introduce pure and extended CNA, ending with the introduction of four fundamental centralities, namely degree, betweenness, closeness, and efficiency.

3.1.1. Pure complex network method

In pure CNA, components schematize buses in nodes and transmission lines in edges, as illustrated in Fig. 4. However, it neglects weight and direction; all the nodes and edges are identical [125].

Two groups of centralities exist in complex network theory. The first one calculates the closeness of nodes/edges to each other, e.g. degree and closeness centralities. The second group evaluates the tie between nodes/edges, e.g. efficiency (shortest path) or flow betweenness centralities [128]. Some metrics also try to merge both groups, e.g. delta centrality (or Δ centrality) [129] and combined degree–betweenness centrality [130]. We introduce the fundamental centralities below. For an in-depth description, the reader can refer to references [118-124, 131] and Table 3.

***Degree*:** The degree of a node goes from 0 (if it is isolated), to k (if it is connected to k nodes of the network). The degree probability distribution of all nodes expresses the topological features of a network. For example, some networks have a node degree distribution that follows a power law as in Eq. (3.1) [132, 133]:

$$P(k) \sim k^{-\gamma}, \quad \gamma > 1 \tag{3.1}$$

where *P(k)* denotes the probability that a randomly selected node has a degree of k, and γ is a constant. With this specific distribution, a few nodes possess a high number of links, i.e. they form hubs. This type of network, namely "scale-free" [20, 134], are particularly vulnerable to intentional attacks but robust to random failures [135]. Other generic networks follow an exponential distribution as in Eq. (3.2):

$$P(k) \sim e^{-k/\tau} \tag{3.2}$$

This is the case of the random graph model [136] and the small-world model [137]. Power grids have the features of a small-world network because they form many clusters with a relatively small path length [84].

***Closeness*:** The closeness centrality sums all the shortest paths of a node. It quantifies how fast the injected information spreads in the network [2].

***Betweenness*:** It measures the ratio and the total number of shortest paths in a graph. Nodes with high values of betweenness can control or regulate information flowing within a network [2].

***Efficiency*:** Efficiency assumes that the load of transmission (electricity, information, packets, gas, water, and so on) between two nodes is proportional to the reciprocal of their distance [20, 138].

Table 3 presents the mathematical definitions of these centralities,

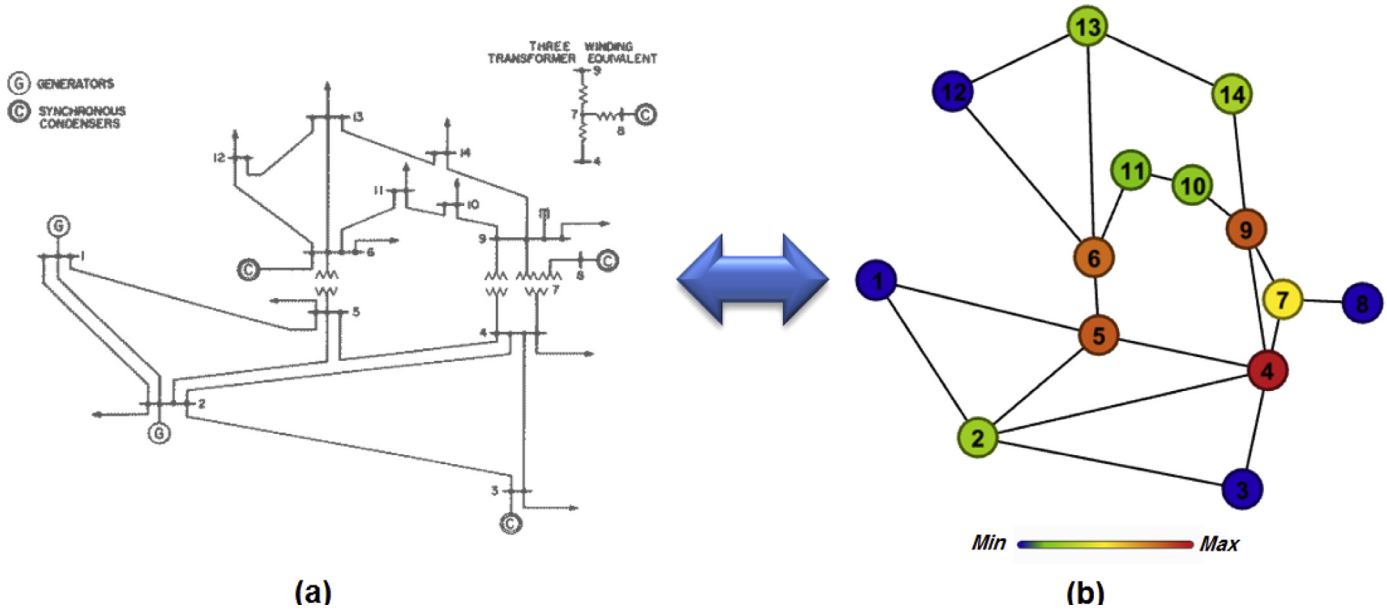

Fig. 4. (a) IEEE-14 test case [126], (b) undirected, unweighted, and pure representation of its related complex network using Gephi (an open source software) [127]. The color scale and the numbers in the nodes provide the betweenness centrality.

Table 3
Some pure centralities in complex network theory and related extended metrics.

pure methods No.	Centrality	Formula	extended methods No.	Centrality	Formula	Ref.
1	Degree	$\frac{\sum a_{ij}}{N-1}$	1	Reliability-based degree	$\frac{\sum a_{ij} \sum p_{ij}}{(N-1)^2}$	[91, 144]
			2	Power-based degree	$\frac{\sum P_{ij}}{N-1}$	[145]
2	Closeness	$\frac{N-1}{\sum d_{ij}}$	3	Reliability-based Closeness	$\frac{N-1}{\sum rd_{ij}}$	[91]
3	Betweenness	$\frac{1}{(N-1)(N-2)} \sum_{i \neq j \neq k} \frac{n_{jk}(i)}{n_{jk}}$	4	Electrical Betweenness	$\sum_{i \neq j \neq k} \frac{P_{jk}(i)}{P_{jk}}$	[91, 116, 145]
4	Efficiency	$\frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{d_{ij}}$	5	Reliability-based Efficiency	$\frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{rd_{ij}}$	[91]
			6	Net ability	$\frac{1}{N_g N_d} \sum_g \sum_d C_g^d \frac{1}{Z_e^{gd}}$	[21, 125, 146]

G: the graph descriptive of the structure of the real network with N nodes, $\boldsymbol{i, j, k \in G}$, $\boldsymbol{p_{ij}}$: the overall probability of connection from node i to node j, $\boldsymbol{a_{ij}}$: is 1 if node i is connected to node j, 0 otherwise, $\boldsymbol{rd_{ij}}$: the most reliable path connecting node i to node j, $\boldsymbol{d_{ij}}$: the shortest path from node i to node j, $\boldsymbol{n_{jk}(i)}$: the number of shortest paths that contain i; $\boldsymbol{n_{jk}}$: the number of shortest paths from node k to node j, $\boldsymbol{P_{ij}}$: power flowing in the line connected in between nodes i and j; $\boldsymbol{P_{jk}}$: the maximum power flowing in the shortest electrical path between buses j and k, $\boldsymbol{P_{jk}(i)}$: the maximum of inflow and outflow at bus i within the shortest electrical path between buses j and k, $\boldsymbol{N_g}$and $\boldsymbol{N_d}$: the numbers of generation and load buses, respectively, $\boldsymbol{Z_e^{gd}}$: an equivalent impedance from a generation bus g to a load bus d as the impedance between the two buses, $\boldsymbol{C_g^d}$: the transfer capacity of the transmission network from generator *g* to load *d*.

as well as those considered in extended CNA.

3.1.2. Extended complex networks methods

Conventional CNA ignores the physical properties, electrical characteristics, and operational limits of power grids. It limits the scope of the analysis [125, 137, 139]. Binary entities hardly represent the real world [140], as lines have different materials, voltage levels, impedances, and related losses. The graph must be weighted to consider such specificities as well as nodes differences [59]. An improvement required to simulate active and reactive power flows, which are governed by Kirchhoff's law and the topology of the network. In addition, directed edges allow simulating the power flow direction, voltage magnitudes, and angles [20].

Scholars have updated the "pure" centralities to take these "extended" characteristics into account. Some studies consider the physical resistance and impedance of lines and cables as the weight on the edges [20, 141]. Others introduce the reliability characteristics of a power transmission system [142]. Weight or P-Q network decomposition [59] features active power flow and the capacity of the generator and the load [2, 125, 143]. Table 3 presents prominent mathematical definitions of metrics in the pure and extended methods. This table highlights how extended centralities are derived from pure ones. In addition, the most important components of the studied papers are categorized in Table 4.

3.2. Flow-based methods

Complex network methods originally ignored the physics of the power system operation, an issue that was partially overcome with extended CNA. Nevertheless, power flow-based methods intrinsically consider physical features [1, 184]. They simulate power flows in power system planning and operations [185] with deterministic and probabilistic approaches, both described in the following subsections.

3.2.1. Deterministic flow-based approach

Power or load flow studies calculate the steady-state solutions of the power system. In a deterministic approach, the modeler/operator knows the injected active powers (P_i) at all buses (N) except the slack

Table 4
Literature on complex network analysis.

Year	Metrics / indicators	Assumptions and Failure Scenarios/ Proposed capability*					Case Study Dimensions*			Reference
		W or U	P or E	Type	Node	Line	Number of nodes	Number of links	Name	
2005	Global efficiency	U	P	PA	YN	Y	98, 146, 127	175, 223, 171	Spanish PG, French PG, Italian PG	[147]
2006	Clustering coefficient, degree distribution, and average path length	U	P	R,PA	Y	Y	4,789, 4,941	5,571, 6,594	Nordic PG, Western U.S. PG	[148]
2007	Weighted line betweenness	W	E	R,PA	N	Y	39, 3,315	46, 3,142	I39, Huazhong-Chuanyu PG	[149]
2007	Clustering coefficient	U	P	R,PA	Y	N	> 3,000 nodes	up to 4,300	UCTE	[93]
2008	Electrical betweenness	B	B	NS	Y	N	300	411	I300	[135]
2008	Topological and reliability efficiency	B	B	R,PA	Y	Y	14	20	I14	[150]
2009	Entropic degree and net-ability	B	B	NS	Y	Y	34, 521	54, 679	I34, Italian PG	[125]
2009	Degree, closeness, betweenness, information, and reliability centralities	B	B	NS	Y	N	14	20	I14	[144]
2009	Efficiency and net-ability	B	B	NS	N	Y	30, 57	41, 78	I30, I57	[146]
2009	Clustering coefficient, information and edge betweenness centrality	B	P	NS	Y	Y	–	6–291	Evolution of French 400-kV PG (1960–2000)	[151]
2009	Complex network analysis and object-oriented modeling	B	B	R,PA	Y	Y	161	219	The Swiss high-voltage PG	[152]
2009	Average and damaged efficiency	B	B	R,PA	Y	Y	14, 300	20, 411	I14, I300	[153]
2010	Developed betweenness index	W	E	NS	Y	N	14	19	I4	[59]
2010	Topological, flow [115], and random betweenness centralities	W	E	NS	Y	N	14	20	I14	[154]
2010	Electric and topological betweenness	B	B	PA	Y	Y	300	409	I300	[155]
2010	Parallel betweenness centrality	W	E	NS	N	Y	14,090, 46,010, 92,370, 172,930	17,346, 57,323, 116,980, 220,648	14,000-bus, 46,000-bus, 90,000-bus, 170,000-bus	[156]
2010	Electrical and topological betweenness centralities	B	B	NS	Y	Y	2935, 300	6567, 409	NYISO-2935 system, I300	[157]
2010	Clustering coefficient, efficiency, and the max indicator of power supply	B	B	R,PA	Y	N	320	441	regional PG in China	[158]
2010	Characteristic path length, connectivity loss, blackout sizes	B	B	R,PA	Y	N	300, 336–1473	409[155], -	I300, 40 areas within the Eastern U.S. PG	[159]
2010	Net-ability, paths redundancy, and survivability	B	B	R,PA	YN	Y	30, 118, 300, 521	41[146], 179 [160], 409[155], 679	I30,, I118, I300, Italian PG	[161]
2011	Electrical closeness and betweenness centralities	W	E	NS	Y	N	5	7	I5	[116]
2011	Electrical betweenness, loss of load index	W	E	R,PA	Y	N	118 [160], 138	179 [160], -	I118, Central China PG	[162]
2011	State transition graph [163] and characteristic length	W	E	NH,PA	Y	Y	118	More than 180	118-bus PG China	[78]
2011	Extended betweenness and net-ability	B	B	PA	Y	Y	118, 300, 521	179, 409, 641	I118, I300, Italian PG	[164]
2012	Structural vulnerability, contingency vulnerability and operational vulnerability indices	W	E	NS	N	Y	93	124	93-bus with DG	[143]
2012	Degree, reliability degree, electrical degree, electrical reliability degree	B	B	NS	Y	Y	24	38	I96	[142]
2012	Degree and betweenness indices	W	P	R,PA	Y	N	118, 4,941	179, 6,594	I118, U.S. PG	[160]
2012	Power flow and random flow betweenness centralities	W	E	R	Y	N	14	20	I14	[165]
2012	Topological and extended betweenness centralities	B	B	R,PA	N	Y	521	641	Italian PG	[166]
2013	Modified pair dependency, closeness and betweenness	B	B	R,PA	Y	N	13, 68, 140, 145	12, 86, 233, 453	4-, 16-,48-, 50-Generators	[2]
2013	Purely topological model, betweenness-based model and direct current power flow model	B	B	NS	Y	Y	57[146], 118 [160], 300[155]	78[146], 179 [160], 409[155]	I57, I118, I300	[54]
2013	Energy-based centrality	W	E	NS	Y	Y	14	20	I14	[167]
2013	Network efficiency and betweenness	U	P	R,PA	Y	N	295	413	Huazhong PG, China	[168]
2013	Local load-redistribution, the normalized avalanche size	W	E	R	Y	N	572	871	Indian PG	[169]
2013	Clustering coefficient, mean shortest path length, degree distribution	U	P	R,PA	N	Y	105	142	Iranian 400-KV PG	[170]
2014	Combined degree-betweenness index	U	P	R,PA	YN	Y	118 [171]	179 [171]	I118	[130]
2014	Degree, betweenness, information, efficiency and closeness and their new reliability-based ones	B	B	R,PA	Y	N	105	142	400-KV PG (IRAN)	[91]
2014	Blackout size and connectivity loss indices	B	B	PA	Y	Y	57[146], 118 [160],300[155]	78[146], 179 [160],409[155]	I57, I118, I300	[85]
2014	Efficiency, source–demand considered efficiency, connectivity level, clustering coefficient, and power supply	B	B	NH,PA	Y	Y	57[146], 118 [160], 300[155]	78[146], 179 [160], 409[155]	I57, I118, I300	[172]
2014	Clustering coefficient	W	E	R	Y	Y	84	200	Floridian high-voltage PG	[173]
2014	Effective graph resistance	W	E	R,PA	N	Y	118 [160], 30[146]	179 [160], 41[146]	I118, I30	[40]

(*continued on next page*)

Table 4 (*continued*)

Year	Metrics / indicators	Assumptions and Failure Scenarios/ Proposed capability*					Case Study Dimensions*			Reference
		W or U	P or E	Type	Node	Line	Number of nodes	Number of links	Name	
2014	Largest component size, connectivity level, DC power flow model, largest attack efficiency	B	B	R,PA	Y	Y	300	409	I300	[57]
2014	Power transfer distribution factors, extended betweenness, net-ability, risk graph	W	E	PA	Y	Y	57, 118, 2,383	80, 179, 2,896	I57, I118, Polish PG	[174]
2014	PageRank algorithm	B	B	PA	Y	N	118	179	I118	[175]
2015	Degree and betweenness-based method	B	B	R,PA	Y	Y	10–884	9–1,059	Dutch medium and low voltage networks	[141]
2015	Net-ability, electrical betweenness and entropy degree	B	B	PA	Y	Y	300	409	I300	[21]
2015	local load-redistribution, the normalized avalanche size	W	P	PA	Y	N	4,941	6,594	Western U.S. PG	[176]
2015	Degree centrality, electrical degree centrality, betweenness centrality and electrical betweenness centrality	B	B	NS	Y	Y	9, 16, 33, 65, 107	10, 20, 41, 96, 171	BPTS 9, BPTS 16, BPTS 33, BPTS 65, BPTS 107	[177]
2015	Grid vulnerability index (GVI), Efficiency-based vulnerability index	W	E	NS	Y	N	57	78	I57	[178]
2016	Pseudo-Laplacian, pseudo-adjacency, pseudo-degree matrices, susceptance-based degree, modified susceptance-based degree, power traffic degree, and power loss degree centrality	B	B	R,PA	Y	N	30[146], 57[146], 300[155], 4,941	41[146], 78[146], 409[155], 6,594	I30,I57, I300, WSCC 4941-bus USA	[8]
2016	Ratio of post-event and pre-event total generator nodes and active power	B	B	R,RA	Y	Y	417	551	Harris county, USA	[27]
2017	A model based on co-citation (MBCC)-hypertext induced topic selection (HITS) algorithm (MBCC−HITS algorithm)	W	E	NS	Y	N	14, 118	20, 179	I14, I118	[179]
2017	Line-graph-based model, bus-based model	U	P	R,PA	Y	Y	14, 30, 57, 118, 300, 4,941	20, 41, 78, 179, 409, 6,594	I14, I30, I57, I118, I300,WECC(USA)	[180]
2017	Motif-based analysis	U	P	PA	Y	N	417, 254, 647, 461, 79, 190, 193, 63	537, 357, 880, 664, 80, 224, 252, 82	Germany, Italy, France, Spain, TenneT, RTE, Amprion, 50 Hertz	[181]
2017	Three node-based measures and three network-based measures	U	P	R,PA	Y	N	2,083	2,571	South Korean PG 3.3–765 KV	[171]
2017	Efficiency, source–demand-considered efficiency, largest component size, connectivity level, and clustering coefficient	B	B	RA	Y	Y	295	413	Central China PG	[182]
2017	Power flow index, vulnerability index, electric closeness	W	E	NS	N	Y	30	42	I30	[183]

* B: Both, P: Pure, E: Extended, W: Weighted, U: Unweighted, Y: Yes, YN: Yes (not shown), N: NO, R: Random failure, PA: Pointwise attacks, RA: Regional attacks, NS: No scenario (all lines or/and all buses or/and N-1 security criterion), NH: Natural hazard (seismic, Hurricane etc.), UCTE: Union for the Coordination of Transmission of Electricity, PG: power grid, IX: IEEE X-bus.

bus, i.e. the other (N-1) buses, the injected reactive powers (Q_i) at all load buses (PQ buses), and the voltage magnitude (V_n) at all generator buses (PV buses) [54]. P_i and Q_i can be expressed in terms of unknown and known state variables as follows:

$$P_i = f_i(\delta_1, \delta_2, \delta_3 ... \delta_n, V_1, V_2, V_3 ... V_n) \quad (3.3)$$

$$Q_i = g_i(\delta_1, \delta_2, \delta_3 ... \delta_n, V_1, V_2, V_3 ... V_n) \quad (3.4)$$

where $i = 1, 2, 3, \ldots, n$, n being the number of buses in the system.

According to Eqs. (3.3) and (3.4), the injected active and reactive powers are functions of voltage magnitudes (V_i) and angles (δ_i) of all buses. These alternative current (AC) power flow equations are non-linear. Therefore, iterative numerical solutions must be used, such as the Gauss–Seidel, Newton–Raphson, or the decoupled power flow methods. These equations and their solutions are detailed in books on electrical power systems [186-188].

Solving AC power flow equations causes a significant computational burden. The direct current (DC) approach limits this issue by linearizing the equations and is required in large-scale simulations or when analyzing many failure scenarios [189]. It considers active powers but ignores reactive powers and transmission losses [190]. Its efficiency approximates the AC power flow, without being iterative and complex [54, 189]. It misrepresents transmission line flows by less than 5%, while being 7 to 10 times faster than the exact solution provided by the AC load flow approach [40]. The estimation is even more accurate in high-voltage low-load power grids [190].

Both power flow approaches are applied to vulnerability analysis. Yan et al. [154] compare a modified DC power flow-based cascading failure simulator using transient stability analysis (TSA). Cavalieri et al. [24] contrast AC power flow-based approach with hierarchical and topological methods. Cascading failures and blackouts were assessed with the Oak Ridge–PSERC–Alaska (OPA) model [42, 191] that uses the DC power flow equation. It solves power flow models under restriction conditions while minimizing the cost function. Nevertheless, the small number of nodes and controlling parameters limit the scope of this model [55]. The University of Manchester developed an AC power blackout model [192] that can consider the cascading failure of transmission lines, post-contingency dispatching of active and reactive powers, or load shedding to prevent a complete blackout. Finally, the CASCADE model [193] describes qualitatively the nature of cascading failure in power systems. However, it ignores the times between adjacent failures and generation re-dispatching during failure [194, 195].

Some studies apply the maximum flow theorem, a deterministic method [140, 196]. It identifies the maximum power flow that a power system can withstand [184]. It works well with weighted networks such as electrical power systems, communication networks, or computer networks. It maximizes the flows from the source to the sink in a network [140, 196]. The maximum flow theorem observes limits similar to that in the power flow calculation, because power grids usually function within capacity and design limitations [6]. Transmission line capacities, bus voltage levels, and generator output greatly influence the power flows. Therefore, the system's state can become abnormal with small perturbations [197].

Various vulnerability analyses of power grids have applied the maximum flow theory. Dwivedi and Yu [88] proposed a maximum-flow-based complex network version. Fan et al. [197] employed the maximum flow theorem to investigate the robustness of a power grid with a tunable load distribution parameter. Fang et al. [198] recently innovated with a multisource multisink problem. They connected virtual nodes to source and sink nodes. Then, all virtual components were connected to a new virtual one. Table 5 will further compare different works based on power flow and maximum flow modeling.

3.2.2. Probabilistic flow-based approach

Uncertainties are ignored in deterministic power flow methods. They require fixed values of load, generation, and transmission line conditions, which are relevant for cases with minimal changes [185, 199, 200]. Probabilistic approaches are preferred when there are large variations of load demand, network configurations, and rates of generator outages or generation, as with wind power. These methods evaluate the system vulnerability according to the uncertainty level [201].

Power system uncertainties can apply both Monte Carlo simulations and analytical methods [200, 202]. Different analytical probabilistic load flow algorithms exist, such as linear approximation, point estimate method, combined cumulants and Gram–Charlier expansions, statistical least square estimation and Nataf transformation, and Latin hypercube sampling [185, 199, 203]. They all linearize the AC power flow equations but use probabilistic density function instead of assuming fixed inputs [199, 200].

Table 5 concludes this section about deterministic and probabilistic flow-based approaches. It summarizes the studies that applied these approaches in vulnerability analysis.

3.3. Logical methods

3.3.1. Game theory

Von Neumann [219] developed the game theory to analyze strategic behavior [220]. Recently, infrastructure security research applied this method in the context of electricity grids [221], transportation networks [222], and supply chains [223]. It deals with intentional attacks and intelligent threats [224] by simulating the behavior of the players, e.g. infrastructure operators and attackers. They reach the Nash equilibrium, if it exists. It occurs when no players can gain to unilaterally change his/her strategy, while others keep their strategies [225]. Non-cooperative games perfectly model strategic interactions between defenders and attackers in malicious attacks. Indeed, each player maximizes his payoff functions, such as the expected damage and the energy loss, independently of the strategy of the other players [220, 226]. Particularly, the Stackelberg strategy as a leader-follower (sequential) game model is recently deployed for modeling security problems [227, 228]. Table 6 will present some applications of game theory.

3.3.2. Hierarchical method

Clustering gathers similar or closely related components together. Dissimilar elements are put in new clusters [229]. The diagram of all clusters is called the hierarchical model of the system [230]. It represents the different levels of the internal related elements in a system. It helps in identifying the critical elements in different potential failure scenarios [229]. Fig. 5 illustrates hierarchical clustering, where the similarity criterion is the distance between the nodes. Fig. 5(a) is the tree of clusters for the network illustrated in Fig. 5(b). This method reduces the computational cost by changing the level of detail of the analysis [231, 232].

Vulnerability analysis considers various hierarchical methods such as the graph representation [19], clustering [229], and logic-based hierarchies [233]. They support both a qualitative and quantitative analysis of CIs [19]. Schaeffer [234] synthesizes a systematic review of this approach.

3.4. Functional methods

3.4.1. Agent-based modeling

Agent-based modeling describes complex systems. It simulates the behavior of the actors, referred to as agents, to determine their impact on the whole system. Each individual acts according to predetermined rules modeled with a set of if-then relationships or decision trees. Probabilistic models can simulate probable heterogeneity of agents' responses/reactions [237]. Agent-based modeling supports systematic analysis, both conceptually and computationally. It applies to contamination in a water distribution system [237], modeling a local multicarrier energy network [238], resilience analysis [239], dynamics

Table 5
Literature on flow-based methods.

Year	Approach	Assumptions and Failure Scenarios/ Proposed capability*					Case Study Dimensions*			Reference
		W or U	P or E	Type	Node	Line	Number of nodes	Number of links	Name	
2010	Probabilistic, combined cumulants and Gram–Charlier Expansions	W	E	R	Y	Y	~16,000	~17,000	Western North American PG	[201]
2010	DC power flow method, error and attack tolerance methodology (degree and betweenness)	B	B	R,PA	Y	Y	118	186	I118	[56]
2010	Deterministic, max-flow theorem	W	E	PA	N	Y	39	–	I39	[204]
2011	Maximum flow algorithm, network efficiency, and flow betweenness	W	E	PA	Y	Y	5, 30[146]	7, 41[146]	I5, I30	[205]
2013	Deterministic, power flow models, ORNL–PSerc–Alaska (OPA) model	B	B	R	Y	Y	300, 300, 300, 418, 400	–	I300, SCALE300, ER300, I418, and SCALE400	[194]
2013	Deterministic, max-flow theorem	W	E	R,PA	N	Y	118	186	I118	[88]
2013	Power flow modeling, eccentricity, radiality, betweenness, centroid, degree centralities	B	B	R,PA	Y	Y	242	310	Swiss PG	[7]
2014	Deterministic, max-flow theorem	W	E	PA	N	Y	14	20	I14	[206]
2014	global efficiency (average efficiency), DC power flow method	B	B	R,PA	Y	N	14, 118	20, 186	I14, I118	[207]
2014	Deterministic, AC power flow, and hierarchical and topological methods	B	B	NH	Y	Y	118	186	I118	[24]
2015	Deterministic, DC power flow	W	E	NS	Y	Y	39, 68	46, 86 [208]	I39, I68	[190]
2015	Deterministic, flow models	B	B	R	Y	Y	24	38	I24	[189]
2013, 2015	Efficiency, connectivity of the network index, load shedding index, severity index, geodesic strength, and power flow modeling	B	B	R,PA	Y	N	5, 14, 24, 30, 57, 118, 300	7[205], 20[165], -, 41[146], 78[146], 179 [160], 409[155]	I5, I14, I24, I30, I57, I118, I300	[209, 210]
2015	AC power flow, bilevel optimization	W	E	PA	Y	Y	118, 2,383	186, 2,896	I118, Polish 2383-bus system	[211]
2015	DC power flow method	W	E	PA	N	Y	57, 118, 247	78[146], 179 [160], -	I57, I118,, I247	[212]
2016	Max-flow theorem and electrical efficiency	W	E	R,PA	N	Y	9, 118 [160]	9, 179 [160]	I9, I118	[184]
2016	Deterministic, max-flow theorem	W	E	PA	Y	N	90	128	500-kV China PG	[197]
2016	Deterministic, max-flow theorem	W	E	PA	N	Y	–	–	Danish PG	[198]
2016	Linear DC optimal power flow (OPF), static performance indices (SPI), and dynamic performance indices (DPI)	W	E	NS	Y	N	43	–	Brazilian Birds test system	[213]
2016	Deterministic, power flow	W	E	NH, R,PA	Y	Y	24[214]	38[214]	I24 [214]	[3]
2016	Maximum flow network algorithm	W	P	NH	N	Y	20,000	–	Entergy power system (USA)	[215]
2017	AC-based power flow	B	B	PA	Y	Y	30, 57, 118	41[146], 78[146], 179 [160]	I30, I57, I118	[216]
2017	Power flow entropy, flow betweenness	W	E	PA	N	Y	39	–	I39 integrated with a 75-MW wind farm	[217]
2017	AC power flow, net-ability, and node electrical centrality	W	E	NS	Y	N	30, 57	41[146], 78[146]	I30, I57	[218]

* B: Both, P: Pure, E: Extended, W: Weighted, U: Unweighted, Y: Yes, N: NO, R: Random failure, PA: Pointwise attacks, RA: Regional attacks, NS: No scenario (all lines or/and all buses or/and N-1 security criterion), NH: Natural hazard (seismic, Hurricane etc.), IX: IEEE X-bus.

Table 6
Literature on logical methods.

Year	Approach	Assumptions and Failure Scenarios/ Proposed capability*					Case Study Dimensions*			Reference
		W or U	P or E	Type	Node	Line	Number of nodes	Number of links	Name	
2007	Game theory	W	E	R,PA	Y	Y	–	–	Swedish PG	[226]
2009	Game theory, zero-sum game, and the mixed-strategy equilibrium	W	E	PA	Y	Y	24	38	I24	[220]
2011	Fault chain theory	W	E	R,PA,RA	N	Y	14	20	I14	[235]
2013	Hierarchical modeling by recursive unsupervised spectral clustering	W	P	R,PA	N	Y	127	171	380-KV Italian PG	[117]
2015	Hierarchy-based approach, node traffic, node betweenness, and node degree	B	B	NH	Y	N	118	186	I118	[231]
2015	Game theory, a discrete simultaneous game, and the mixed-strategy equilibrium	W	E	PA	N	Y	73	117	IEEE RTS 96	[236]
2016	Hierarchical graph representation and clustering and Monte Carlo simulation	W	E	R	Y	Y	114	112	I123 bus	[19]
2016	Game theory, power flow and topological analysis	B	B	PA	N	Y	30	42	I30	[221]

* B: Both, P: Pure, E: Extended, W: Weighted, U: Unweighted, Y: Yes, N: NO, R: Random failure, PA: Pointwise attacks, RA: Regional attacks, NS: No scenario (all lines or/and all buses or/and N-1 security criterion), NH: Natural hazard (seismic, Hurricane etc.), IX: IEEE X-bus

calculations [240], and simulation of large-scale electric mobility [241].

Several programming environments implement and test agent-based models. For instance, JADE, a Java-based platform, models microgrid, electric vehicle management system, fault detection, protection, and self-healing [242]. The U.S. Pacific Northwest National Laboratory (PNNL) has recently developed VOLTTRON in Python [243, 244]. It considers various programming languages, unlike other models, and can support fault detection, renewable energy integration, smart monitoring and diagnostic systems [245]. Particularly, Sujil et al. [242] introduce different platforms for agent-based modeling.

3.4.2. Dynamic modeling

Great disturbance generates a large magnitude of transient energy. For instance, the kinetic energy of generator rotors will be converted to potential energy in the power system. If the power system cannot absorb and control this energy, it will lose its stability [246]. Different time domain [186] and direct methods based on energy functions [247] examine the stability of a power system. The second method [248] performs well in power system dynamics and security analysis [249-253]. For further understanding, Table 7 compares applications of functional methods.

3.4.3. Multi-objective optimization

Multi-objective optimization (MOO) is a mathematical approach to find values of decision variables which correspond to the optimum of more than one objective function [254]. Cho et al. [255] presented the state-of-the-art modeling and techniques such as weighted sum, goal programming, ε-constraints and so on, to solve MOO problems and also, discussed advantages and disadvantages of each modeling and solution technique in detail. Different bi-level (e.g. attacker-defender) and tri-level (e.g. design-attack-defend) frameworks are introduced for vulnerability analysis of different critical infrastructure using MOO [211, 256]. Recently, Faramondi et al. [257] employed MOO in vulnerability analysis of a power system as well as an airline network. They used pairwise connectivity concept (a degree graph based concept). Also, the defined objectives are simultaneously minimizing the degree of connectivity and minimizing the cost of the attack from attacker perspective using MOO.

4. Discussion

4.1. Overview

This paper reviews the most cited and recent papers on vulnerability analysis of power grids. We have summarized them in four tables according to several criteria, such as methodology, assumptions, test cases, failure scenarios, and the proposed modeling capability (node and/or line modeling). They allow readers to grasp the differences, but this section extends the comparison and discussion.

Fig. 6 presents the distribution of the reviewed papers in the last decade according to our categorization. Scholars first applied CNA and functional methods to power system vulnerability analysis. While the number of studies applying the functional approach has been remaining stable, CNA application grew and led the field. Flow-based methods, despite appearing later, seem to attract interest in the past five years. Finally, logical methods are marginally applied.

Fig. 7 provides the distribution of the chosen approaches and the used scenarios. As we already observed in the previous figure, most of the studies applied CN in multiple scenarios. The statistics about the scenarios shows that few papers are devoted to natural hazards. This is surprising given the enormous extent of their impacts, indicating that more studies are required in this area. Finally, we also computed the share of studies that consider generic models (58%), real cases (29%), or both (13%). Generic models provide the opportunity to compare the results and replicate them, possibly explaining the increased interest in

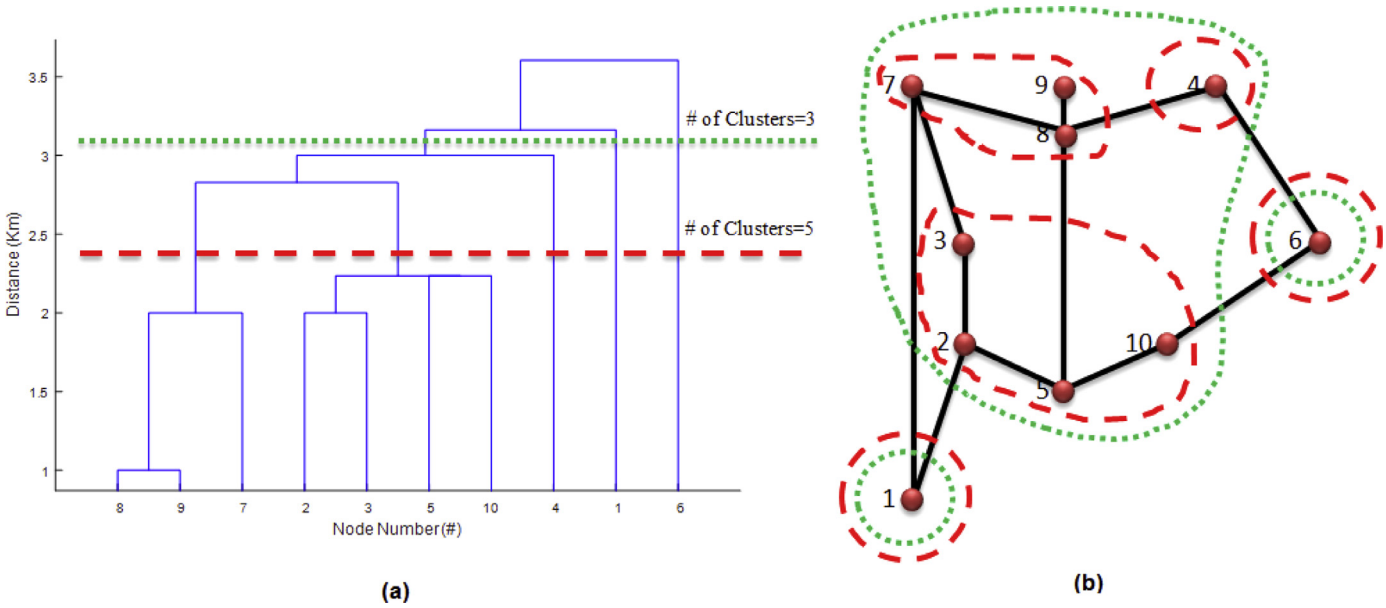

Fig. 5. Illustrative example of hierarchical clustering: (a) a hierarchical clustering dendrogram (a tree of clusters) and two different levels of abstraction (dotted lines) and (b) the network and its clustered nodes.

Table 7
Literature on functional methods.

Year	Approach	Assumptions and Failure Scenarios/ Proposed capability*					Case Study Dimensions*			Reference
		W or U	P or E	Type	Node	Line	Number of nodes	Number of links	Name	
1994	Transient energy function (TEF) method	W	E	NS	Y	N	50	–	I50	[252]
2005	Particle swarm optimization, energy margin	W	E	R	N	Y	179	203	WSCC, U.S.	[258]
2007	Radial basis function, neural network	W	E	R,PA	Y	Y	300	411	I300	[259]
2007	Nonlinear optimization method, power flow	W	E	PA	N	Y	30, 118	41, 179	I30, I118	[260]
2008	Energy model	W	E	R	N	Y	9	–	Three-generator system	[261]
2009	Potential energy model	W	E	NS	N	Y	30	41	I30	[262]
2011	Multi-agent complex network model	W	E	R,PA	Y	Y	2,556	2,892	North China PG	[263]
2012	Energy function, degree index, and vulnerable sensitivity index	W	E	NS	N	Y	30	41	I30	[264]
2014	Transient energy function, complex network model	W	E	NS	Y	Y	~31	–	Six-generator system	[246]
2016	Dynamic model of AC power grids	W	E	R,PA	N	Y	120 236 118	165 320 179	Great Britain HV line, Scandinavia, I118	[265]

* B: Both, P: Pure, E: Extended, W: Weighted, U: Unweighted, Y: Yes, N: NO, R: Random failure, PA: Pointwise attacks, RA: Regional attacks, NS: No scenario (all lines or/and all buses or/and N-1 security criterion), NH: Natural hazard (seismic, Hurricane etc.), IX: IEEE X-bus.

this type of models.

4.2. Comparison of methods

Table 8 maps a chosen method to its respective scenario, although it should be noted that other combinations may also work. Each method possesses its own limitations, implying that the perfect method does not exist. Table 9 helps the reader to understand the advantages and disadvantages of each method. We compare the scalability and the computational burden of the analytical methods according to the case study dimensions (number of simulated nodes and edges). The comparison demonstrates that complex network methods better model larger grids compared to other methods owing to the lesser computational burden.

4.3. Correlation analysis

Spearman's rank correlation coefficient allows comparing the results of different methodologies. It tests the association between two sets of ranked data. The results are always between 1.0 (a perfect positive correlation) and − 1.0 (a perfect negative correlation) [267]. A positive correlation means two variables increase or decrease together. In contrast, a negative correlation means the variables increase/decrease in opposite directions. Herein, the correlation coefficient compares the ranking of critical components using different methods.

Fig. 8 shows the matrix of Spearman's rank correlation coefficient for some available results from only CN approaches, which are the most applied in the field. We consider five works [144, 154, 165, 179, 268], already listed in Table 4, because they used the same IEEE 14-bus generic case study. Three groups appear. First, global topological/reliability efficiency, topological/reliability closeness, and reliability degree are highly correlated at more than approximately 80%. They have a very low (even negative) correlation with power flow betweenness and the MBCC–HITS algorithm. Finally, reliability betweenness, topological degree, and random flow betweenness have a moderate level of positive correlation with the first group. These results show that not all CN approaches have a good correlation to each other, demonstrating a

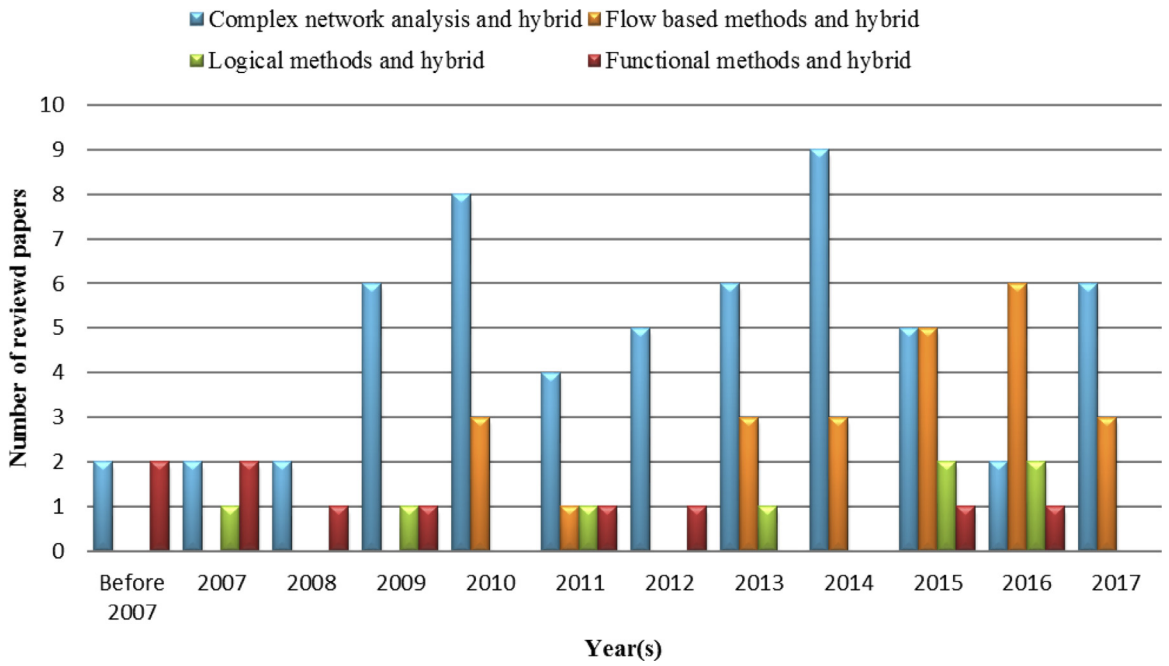

Fig. 6. Number of reviewed papers according to different categories, from before 2007 to 2017.

need for further comparing and even developing new methods and centralities in this field.

Recently, Li et al. and Rocchetta and Patelli [216, 269] presented a similar analysis to show the correlation, but between the power flow approach and CN methods. They demonstrated that a relatively high correlation (0.6–1) exists between AC- and DC-based power flow models. Rocchetta and Patelli [269] also concluded that there is a weak (−1 to 0.3) and moderate (0.3–0.6) correlation between the power flow method and selected CN metrics. Li et al. [216] present the same results between the power flow method and the selected CN metrics but the selected CN metrics are moderately and highly correlated. Particularly, Cortes et al. [231] show that hierarchical method as a logical method shows a higher correlation with power flow results in comparison with CN methods.

However, some studies (e.g. [209, 216]) present a high correlation between CN and other methods but according to Fig. 8 and some articles (e.g. [1, 269]), it is not possible to rely on CN completely. That is why the extended and pure CN methods are currently improving and new centralities are being proposed to consider the realistic properties of networks and operating limits. This improvement in CN centralities may increase its disadvantages (e.g. accuracy) as well as maintain its advantages (e.g. being easy and fast) at the same time.

4.4. Emerging topics and future research work

Based on the literature review and the comparisons, we can point out four emerging topics that require further research efforts.

4.4.1. N-k problem (N-k contingency analysis)

Most power transmission networks fulfill the so-called “N-1 security criterion.” If any single component fails, the loads can be restored without load shedding [12, 262]. However, blackouts often result from cascading failures rather than a single-component failure. Unpredictable combinations of circumstances or inadequate controls can disconnect further lines or nodes [270], jeopardizing the common N-1 (or even N-2) security criteria [5]. Topical research analyzes the N-k ($k \geq 2$) contingency and its impacts on the robustness of the power system [156].

Models cannot consider all combinations of failures. Real systems consist of thousands to tens of thousands of components (N). A single

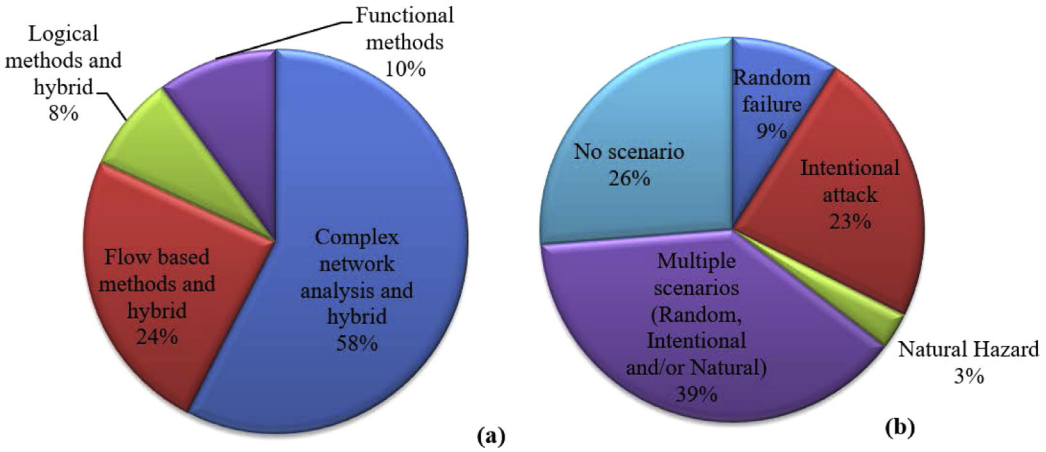

Fig. 7. Distribution of reviewed papers based on (a) approach and (b) scenarios.

Table 8
Methods used for different power system hazards.

Power system hazard		Nature	Scenario basis	Used methods in reviewed papers
Random failure		Accidental/random	Random	Complex network analysis [2, 8, 27, 40, 57, 91, 93, 130, 141, 148-150, 152, 153, 158-162, 165, 166, 168-171, 173, 180] Flow-based methods [3, 7, 56, 88, 184, 189, 194, 201, 207, 209, 210] Logical methods [19, 117, 226, 235] Functional Methods [258, 259, 261, 263, 265]
Natural hazard		Accidental	Hazard maps and affected areas	Complex network analysis [78, 172] Flow-based methods [3, 24, 215] Logical method [231]
Intentional attacks	Pointwise attack	Intentional/strategic	Critical component	Complex network analysis [2, 8, 21, 40, 57, 78, 85, 91, 93, 130, 141, 147-150, 152, 153, 155, 158-162, 164, 166, 168, 170, 171, 174-176, 180, 181] Flow-based methods [3, 7, 56, 88, 184, 197, 198, 204-207, 209-212, 216, 217] Logical methods [117, 220, 221, 226, 235, 236] Functional Methods [259, 260, 263, 265]
	Regional attack	Intentional/strategic	Critical area	Complex network analysis [27, 182] Logical method [235]

failure requires the verification of only N cases. However, an N-k analysis must consider a k-combination from N components [271]. For an illustrative example, using an Opteron processor with 2.2-GHz clock speed, and 3-GB memory per processor, N-2 and N-3 contingency analysis of the IEEE-118 system with 118 nodes will take around 1 day and 65 days, respectively [260]. Fortunately, Li et al. [216] and Rosato et al. [272] show that N-3 analyses suffice to measure the importance of a bus or a branch in a single or coupled networks, and modern algorithmic approaches are promising to investigate the optimal N-k level [216].

4.4.2. Robustness and optimal decision

Many factors affect the development of CI. Economic, political, demographic, social, and technological drivers can cause delay or stop deployment [151]. Operators should consider a holistic perspective, which integrates robustness, resilience, and reliability [273, 274]. It also means computing trade-off between cost and benefits [275]. For instance, small and low-cost changes in power grids can substantially increase robustness [276]. Changing 5.5% and 2% of links could increase the EU power grid's robustness by 45% and 27% [276]. In contrast, installing new lines can decrease the grid's robustness, as presented in the so-called Braess paradox [212].

4.4.3. Technology evolution and emerging threats

The power system is observing various fundamental transformations, which generate vulnerability. We introduce three major threats below.

Prosumers: Most literature focuses on the high voltage level, at which large blackouts happen [13]. However, some studies [141, 277] show that large blackouts could increase with the shift towards distributed generation and prosumers (producers and consumers of energy). The main role of high-voltage grids will change in the future and hence distribution systems must be considered to be at risk and in need of vulnerability analysis.

Prosumers come with the concept of smart grids. A smart grid uses communication technology to improve efficiency, load balancing, and network management [47, 139, 273, 278-281]. It also increases the potential for cyber-attacks and jeopardizes the security of the power system. These changes complicate the analysis and management of the grid [13].

The interdependency and combination of CIs: CIs are becoming increasingly interconnected [282]. An accident in a specific infrastructure, e.g. water and energy, can trigger a cascading failure in the other sectors. For instance, an event in a gas network can cause the shutdown of the gas-fired generators, and in turn in the energy sector. The interdependency significantly affects power security [278]. It requires a holistic analysis, including the nexus perspective.

Climate change and renewable energy: Many countries are engaged in decarbonizing their energy mix, while some are phasing out nuclear energy. Renewable energies are deployed around the world. However, the intermittent forms of renewable energy bring network operators the challenge of balancing production with the real-time demand. This threatens the stability and security of the power system. In particular, extreme weather, which could increase with climate change, can disturb the energy system [278, 283].

Most energy policies aim to increase energy efficiency, thus decreasing energy consumption. However, limiting carbon emissions can actually increase electricity demand. Heat and transport sectors tend to move from fossil fuels to electricity [284]. Therefore, electricity supply and transmission capacity must follow the growing demand to limit threats to the security of power systems.

4.4.4. Hybrid approaches

The growing complexity of some networks jeopardizes the reductionist methods [285]. A holistic approach requires a hybrid one because each method possesses its own limitations. This means the perfect method does not exist, Table 9 shows. An emerging idea is to integrate different methods to obtain better, faster, and more accurate results at the same time. For instance, complex network methods require low computing burden while the power flow method is more accurate but slow. To take advantage of their respective strengths, they can be integrated using “importance and criticality” definitions, as discussed below.

Importance and criticality are two key concepts that should not be confused [286]. The important component in a system possesses a high portion of responsibility (e.g. provides or carries more power in power grids), while the critical components drastically affect the performance of that system if they are disconnected [287]. Fig. 9 presents the differences between these two concepts with a simplified three-line network. Line 2 is always important because it transports a large volume of electricity. However, in **Fig. 9**a, line 2 is not critical. If it is disconnected, the system keeps delivering the full load through lines 1 and 3. In **Fig. 9**b, line 2 is both important and critical because the full load (here 700) can no longer be supplied without it.

Indeed, some centralities such as “degree” and “betweenness” show very well the importance of components but not their criticality. Briefly speaking, for a large network with thousand components, applying a more accurate approach like the AC power flow is impossible. We can apply complex networks to rank the importance of components, and then apply a more accurate approach like the AC power flow to the top important components (e.g. 30% of the top important components in the list) to exactly find the most critical ones, not to all components. In this manner, we can integrate both the approaches.

Table 9
Some major advantages and disadvantages of different methods used in vulnerability analysis.

Methods			Advantages/capability	Disadvantages/limitations	Ref.
Analytical methods	Topological methods	Pure models	• Very fast and simple for calculation of indicators • Scalable and can model small to very big power systems • Can be applied to real-time application because of high computing efficiency	• Neglect the realistic and basic power flow and network constraints and operation • Excessive simplification can lead to inaccurate results. • Not reliable, cannot be used alone for decision-making	[20, 22, 57, 141, 194, 221]
		Extended models	• As above • Consider the realistic and basic power flow and network constraints and operation	• Consider few constraints of the network	[20, 22, 57, 141, 194, 221]
	Flow methods	Deterministic approach	• DC models are computationally efficient. • AC models consider the realistic and basic power flow and network constraints. • The maximum flow theorem is fast and simple for calculation of indicators.	• DC models may fail to simulate the cascading failure. • DC models ignore some network parameters such as the reactive power balance equations, line losses. They also assume that all voltage magnitudes equal one per unit. • DC models misestimate the importance of components. • AC power flow equations cause significant computational burden and have convergence problem.	[216]
		Probabilistic approach	• Can simulate realistic model with uncertainty	• Lower scalability in comparison with topological methods	[194]
	Logical methods	Hierarchical methods	• A clustering algorithm can reduce the dimension of the network. • Can be applied to qualitative and quantitative analysis • Reduce the complexity of the network.	• Cannot model interdependency between networks • Hardly applicable to large power systems • Not flexible; adding or removing the component may change all representations	[19]
		Game theory-based modeling	• Simulate the actions of intelligent adversaries	• Needs probabilities of different consequences (e.g., attack probability or failure) for various possible combinations of players' actions	[25]
	Functional methods	Agent-based modeling	• Can model interactions between network components • Flexibility to add or remove the components • Can consider different environments, as a sublayer of the model • Can model a large-scale complex network with a large number of dynamic and nonlinear interactions	• Large number of required parameters for modeling real systems • High computational burden	[244, 266]
		Dynamic and energy function	• Can simulate a realistic model with its dynamic behavior	• Hardly applicable to large power systems (time domain methods) • Large number of required parameters for modeling real system (time domain methods).	[186]
		Multi-objective optimization	• Achieve the best action in intentional attacks considering different objective functions	• Computationally inefficient without feasible solution space	[255]

Method	Global topological efficiency	Global reliability efficiency	Topological closeness	Reliability closeness	Topological betweenness	Reliability betweenness	Topological degree	Reliability degree	Random flow betweenness	Power flow betweenness	MBCC-HITS algorithm
Global topological efficiency	1.00	0.84	0.93	0.88	0.91	0.55	0.78	0.92	0.65	-1.00	0.38
Global reliability efficiency	0.84	1.00	0.74	0.94	0.84	0.61	0.49	0.82	0.23	-1.00	-0.05
Topological closeness	0.93	0.74	1.00	0.88	0.95	0.54	0.84	0.90	0.69	-0.99	0.44
Reliability closeness	0.88	0.94	0.88	1.00	0.93	0.60	0.62	0.87	0.38	-1.00	0.09
Topological betweenness	0.91	0.84	0.95	0.93	1.00	0.57	0.83	0.91	0.66	-0.95	0.45
Reliability betweenness	0.55	0.61	0.54	0.60	0.57	1.00	0.50	0.64	0.16	-0.94	-0.10
Topological degree	0.78	0.49	0.84	0.62	0.83	0.50	1.00	0.86	0.76	-0.80	0.53
Reliability degree	0.92	0.82	0.90	0.87	0.91	0.64	0.86	1.00	0.60	-0.95	0.25
Random flow betweenness	0.65	0.23	0.69	0.38	0.66	0.16	0.76	0.60	1.00	-1.00	0.88
Power flow betweenness	-1.00	-1.00	-0.99	-1.00	-0.95	-0.94	-0.80	-0.95	-1.00	1.00	0.88
MBCC-HITS algorithm	0.38	-0.05	0.44	0.09	0.45	-0.10	0.53	0.25	0.88	0.88	1.00

Fig. 8. Matrix of Spearman's rank correlation coefficient for some CN approaches using the same test case (IEEE14).

5. Conclusions

Literature on vulnerability analyses of CI incessantly grows. Scientists innovate in this field, and this review provides a snapshot of the current state-of-play. New approaches will emerge in the coming years. Unavoidably, this review should be continued in the future. Nevertheless, we trust it will remain relevant for a while for two main reasons.

First, this paper filled a gap in other published reviews. It provided a broad overview of the methods, rather than focusing on a specific one. We devoted substantial effort in summarizing, categorizing, and identifying the strengths of each analytical method. The paper therefore guides the reader through this field of research, as illustrated in Fig. 3. We also focused on three classes of events, namely natural hazards, intentional attacks, and random failures (Fig. 1) that will help scholars determine the relevant application of the various methods available, including emerging methods. Finally, we provided and compared various relevant definitions of vulnerability. They cover a broad set of interpretations, which are unlikely to evolve significantly.

Second, scientists are currently innovating with hybrid approaches. Ongoing research focuses on integrating the above-presented methods, rather than developing new ones. With AI and deep learning, new boxes could emerge in Fig. 3. However, knowing and comparing the established methods can support scholars in choosing more relevant integrative approaches.

This paper summarized about 100 papers in the tables and reviewed totally about 300 articles. Rather than providing a take-home message, we recommend keeping in mind Table 9. It summarizes the advantages and disadvantages of the standard methods in vulnerability analysis. It highlights that no modeling approach can investigate all aspects of this field. In fact, the appropriate model depends on the type of event and the specific case study. Thus, this paper contributes to guiding the reader in this fascinating and topical field.

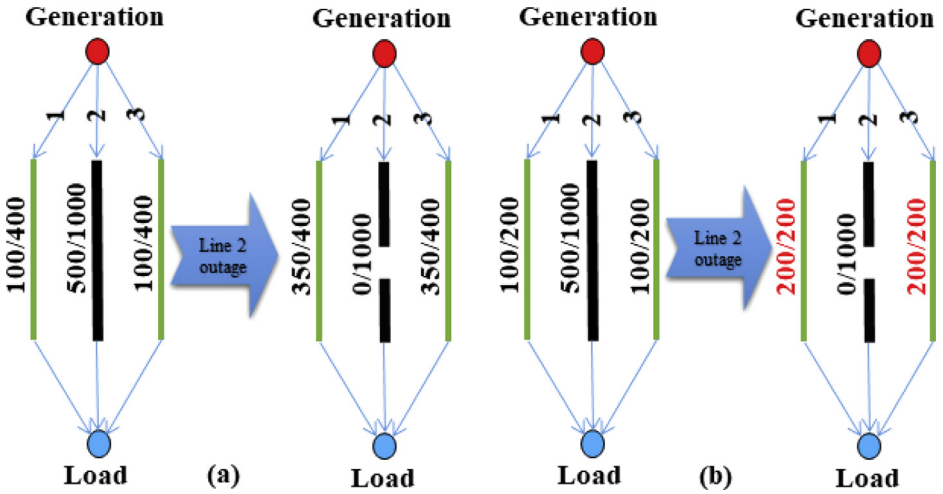

Fig. 9. Important vs. critical components: (a) line 2 (black line) is an important component but not a critical one (b) line 2 (black line) is an important as well as a critical component (x/y on the line: x is the operating power and y is the installed capacity).

Acknowledgment

The authors thank three anonymous referees for their very useful and relevant comments. The first author acknowledges the support of Iran's Ministry of Science and Technology and Schmidheiny Foundation. The second author thanks the Swiss National Foundation for funding his research with the project entitled "Robust decision-making in the electricity sector."

References

[1] Zio E. Challenges in the vulnerability and risk analysis of critical infrastructures. Reliab Eng Syst Saf 2016;152:137–50.
[2 Gutierrez F, et al. Vulnerability Analysis of Power Grids Using Modified Centrality Measures. Discrete Dyn Nature Soc 2013.
[3] Akdeniz E, Bagriyanik M. A knowledge based decision support algorithm for power transmission system vulnerability impact reduction. Int J Electr Power Energy Syst 2016;78:436–44.
[4] Sweeney JL. The california electricity crisis. Stanford, Calif.: Hoover Institution Press; 2002.
[5] Mao A, Yu J, Guo Z. Electric power grid structural vulnerability assessment. 2006 IEEE Power Eng Soc General Meeting 2006.
[6] Pant R, Hall JW, Blainey S. Vulnerability assessment framework for interdependent critical infrastructures: case-study for Great Britain's rail network. Eur J Transp Infrastruct Res 2016;16(1):174–94.
[7] Bilis EI, Kroger W, Nan C. Performance of Electric Power Systems Under Physical Malicious Attacks. IEEE Syst J 2013;7(4):854–65.
[8] Chopade P, Bikdash M. New centrality measures for assessing smart grid vulnerabilities and predicting brownouts and blackouts. Int J Critical Infrastruct Prot 2016;12:29–45.
[9] Bompard E, et al. 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.
[10] Veloza OP, Cespedes RH. Vulnerability of the Colombian electric system to blackouts and possible remedial actions. 2006 IEEE Power Eng Soc General Meeting 2006.
[11] Kamali S, Amraee T. Blackout prediction in interconnected electric energy systems considering generation re-dispatch and energy curtailment. Appl Energy 2017;187:50–61.
[12] Zio E, Aven T. Uncertainties in smart grids behavior and modeling: What are the risks and vulnerabilities? How to analyze them? Energy Policy 2011;39(10):6308–20.
[13] 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.
[14] Panteli M, Mancarella P. Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies. Electr Power Syst Res 2015;127:259–70.
[15] Bompard E, et al. Classification and trend analysis of threats origins to the security of power systems. Int J Electr Power Energy Syst 2013;50:50–64.
[16] VSE. Wege in die neue stromzukunft gesamtbericht. Aarau: Verband Schweizerischer Elektrizitätsunternehmen (VSE); 2012.
[17] Densing M, Hirschberg S, Turton H. Review of Swiss electricity scenarios 2050. Report prepared for the Group Energy Perspectives and the Swiss Competence Center for Energy Research "Supply of Electricity"(SCCER SoE). PSI Bericht; 2014.
[18] Haidar AMA, Mohamed A, Hussain A. Vulnerability Assessment of Power System Using Various Vulnerability Indices. 2006 4th Student Conference on Research and Development. 2006.
[19] Ferrario E, Pedroni N, Zio E. Evaluation of the robustness of critical infrastructures by Hierarchical Graph representation, clustering and Monte Carlo simulation. Reliab Eng Syst Saf 2016;155:78–96.
[20] Cuadra L, et al. A Critical Review of Robustness in Power Grids Using Complex Networks Concepts. Energies 2015;8(9):9211–65.
[21] Bompard E, Luo L, Pons E. A perspective overview of topological approaches for vulnerability analysis of power transmission grids. Int J Critical Infrastruct 2015;11(1):15–26.
[22] Pagani GA, Aiello M. The Power Grid as a complex network: A survey. Physica a-Stat MechAppl 2013;392(11):2688–700.
[23] Yusta JM, Correa GJ, Lacal-Arantegui R. Methodologies and applications for critical infrastructure protection: State-of-the-art. Energy Policy 2011;39(10):6100–19.
[24] Cavalieri F, et al. Models for Seismic Vulnerability Analysis of Power Networks: Comparative Assessment. Comput-Aided Civil Infrastruct Eng 2014;29(8):590–607.
[25] Bier VM, Azaiez MN. Game theoretic risk analysis of security threats. Int series in operations research & management science vi. New York: Springer Science +Business; 2009. p. 236.
[26] Jamshidi, M., *Systems of systems engineering: principles and applications*. 2009, Boca Raton, Fla.: CRC; London: Taylor & Francis [distributor].
[27] Ouyang M. Critical location identification and vulnerability analysis of interdependent infrastructure systems under spatially localized attacks. Reliab Eng Syst Saf 2016;154:106–16.
[28] Zio E, Piccinelli R, Sansavini G. An All-Hazard approach for the vulnerability analysis of critical infrastructures. Advances in Safety, reliability and risk management. CRC Press; 2011. p. 2451–8.
[29] Wang SL, Hong L, Chen XG. Vulnerability analysis of interdependent infrastructure systems: A methodological framework. Physica a-Stat Mech 2012;391(11):3323–35.
[30] Wang SL, et al. Vulnerability analysis of interdependent infrastructure systems under edge attack strategies. Saf Sci 2013;51(1):328–37.
[31] Agostino GD, et al. Methodologies for inter-dependency assessment. 2010 5th Int Conference on Critical Infrastructure (CRIS). 2010.
[32] Johansson J, Hassel H. An approach for modelling interdependent infrastructures in the context of vulnerability analysis. Reliab Eng Syst Saf 2010;95(12):1335–44.
[33] Wang S, Liu J. Robustness of single and interdependent scale-free interaction networks with various parameters. Physica A 2016(460):139–51.
[34] Griot C. Modelling and simulation for critical infrastructure interdependency assessment: a meta-review for model characterisation. Int J Critical Infrastructs 2010;6(4):363–79.
[35] Huang C-N, Liou JJH, Chuang Y-C. A method for exploring the interdependencies and importance of critical infrastructures. Knowl-Based Syst 2014;55:66–74.
[36] Zio E, Sansavini G. Modeling Interdependent Network Systems for Identifying Cascade-Safe Operating Margins. IEEE Trans Reliab 2011;60(1):94–101.
[37] Eusgeld I, Nan C, Dietz S. "System-of-systems" approach for interdependent critical infrastructures. Reliab Eng Syst Saf 2011;96(6):679–86.
[38] Gao JX, Li DQ, Havlin S. From a single network to a network of networks. Natl Sci Rev 2014;1(3):346–56.
[39] Atputharajah A, Saha TK. Power system blackouts - literature review. 2009 Int Conference on Industrial and Information Systems (ICIIS). 2009.
[40] Koc Y, et al. The impact of the topology on cascading failures in a power grid model. Physica A 2014;402:169–79.
[41] Carreras BA, et al. Critical points and transitions in an electric power transmission model for cascading failure blackouts. Chaos 2002;12(4):985–94.
[42] Dobson I, et al. Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization. Chaos 2007;17(2).
[43] Prieto F, Sarabia JM, Saez AJ. Modelling major failures in power grids in the whole range. Int J Electr Power Energy Syst 2014;54:10–6.
[44] Beck G, et al. Global blackouts–Lessons learned. Power-Gen Europe 2005.
[45] Learning from the blackouts: transmission system security in competitive electricity markets. Paris: Int Energy Agency; 2005.
[46] Eremia, M. and M. Shahidehpour, Handbook Electral power system dynamics: modeling, stability, control.
[47] Huang W, et al. A lesson learned from recent cascading outages: Coupled interface and its impact on the smart-grid development. 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT). 2013.
[48] Gomes P. New strategies to improve bulk power system security: lessons learned from large blackouts. IEEE Power Eng Soc General Meeting, 2004 2004.
[49] Begovic MM. Electrical transmission systems and smart grids: selected entries from the encyclopedia of sustainability science and technology vi. New York: Springer; 2013. p. 324.
[50] Zeng B, et al. An analysis of previous blackouts in the world: Lessons for China's power industry. Renew Sust Energy Rev 2015;42:1151–63.
[51] Lai LL, et al. Lessons learned from July 2012 Indian blackout. 9th IET Int Conference on Advances in Power System Control, Operation and Management (APSCOM 2012). 2012.
[52] United States. Congress. Office of Technology Assessment. Physical vulnerability of electric systems to natural disasters and sabotage viii. Washington, D.C.: Congress of the U.S; 1990. p. 63. For sale by the Supt. of Docs., U.S. G.P.O.
[53] Murray AT, Grubesic TH. Critical infrastructure: reliability and vulnerability. Berlin; London: Springer; 2007.
[54] 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).
[55] Ke S, Zhen-Xiang H. Analysis and Comparison on Several Kinds of Models of Cascading Failure in Power System. 2005 IEEE/PES Transmission & Distribution Conference & Exposition: Asia and Pacific. 2005.
[56] Chen G, et al. Attack structural vulnerability of power grids: A hybrid approach based on complex networks. Physica a 2010;389(3):595–603.
[57] Ouyang M, Yang K. Does topological information matter for power grid vulnerability? Chaos 2014;24(4):043121.
[58] Liu CC, et al. The strategic power infrastructure defense (SPID) system - A conceptual design. IEEE Control Syst Mag 2000;20(4):40–52.
[59] Zhenbo W, Liu J. Research on the electric power grid vulnerability under the directed-weighted topological model based on Complex Network Theory. Mechanic Automation and Control Engineering (MACE), 2010 Int Conference on. 2010.
[60] Huang T, et al. Analysis and Visualization of Natural Threats Against the Security of Electricity Transmission System. Sci Bull Electr Eng Faculty 2017.
[61] Shen B, Koval D, Shen S. Modelling extreme-weather-related transmission line outages. Engineering Solutions for the Next Millennium. 1999 IEEE Canadian Conference on Electrical and Computer Engineering (Cat. No.99TH8411). 1999.
[62] Zhu YH, et al. Resilience Analysis of Power Grids Under the Sequential Attack. IEEE Trans Inf Forensics Secur 2014;9(12):2340–54.
[63] Miller, C.R., *Electromagnetic pulse threats in 2010*. 2005, DTIC Document.
[64] *Terrorism and the electric power delivery system*. 2012, Washington, D.C.: National Academies Press.
[65] Liu Y, Ning P, Reiter MK. False Data Injection Attacks against State Estimation in Electric Power Grids. Acm Trans Inf Syst Security 2011;14(1).
[66] Liu X, Li Z. Local Topology Attacks in Smart Grids. IEEE Trans Smart Grid 2016(99):1–10.
[67] Kim J, Tong L. On Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures. IEEE J Selected Areas Commun 2013;31(7):1294–305.
[68] Liu X, Li ZY. Local Load Redistribution Attacks in Power Systems With Incomplete Network Information. IEEE Trans Smart Grid 2014;5(4):1665–76.
[69] Hug G, Giampapa JA. Vulnerability Assessment of AC State Estimation With Respect to False Data Injection Cyber-Attacks. IEEE Trans Smart Grid 2012;3(3):1362–70.
[70] Chen PY, Hero AO. Assessing and safeguarding network resilience to nodal attacks.

IEEE Commun Mag 2014;52(11):138–43.
[71] Ouyang M, et al. Mitigating electric power system vulnerability to worst-case spatially localized attacks. Reliab Eng Syst Saf 2017;165:144–54.
[72] Pu CL, Cui W. Vulnerability of complex networks under path-based attacks. Physica a 2015;419:622–9.
[73] Wolf S, et al. Clarifying vulnerability definitions and assessments using formalisation. Int J Climate Change Strategies Manage 2013;5(1):54–70.
[74] Dolan M, et al. Forensic Disaster Analysis of Flood Damage at Commercial and Industrial Firms. Flood damage survey and assessment. John Wiley & Sons, Inc; 2017. p. 195–209.
[75] Kundak S. Cascading and unprecedented effects of disasters in urban system. Intelligent systems and decision making for risk analysis and crisis Response.. CRC Press; 2013. p. 743–8.
[76] Pascale S, Sdao F, Sole A. A model for assessing the systemic vulnerability in landslide prone areas. Natural Hazards Earth Syst Scis 2010;10(7):1575–90.
[77] Veen AVD, Logtmeijer C. Economic Hotspots: Visualizing Vulnerability to Flooding. Natural Hazards 2005;36(1):65–80.
[78] Chang L, Wu ZG. Performance and reliability of electrical power grids under cascading failures. Int J Electr Power 2011;33(8):1410–9.
[79] French, G.S. and D. Gootzit, *Defining and Assessing Vulnerability of Infrastructure to Terrorist Attack*, in *Vulnerab, Uncer, Risk*. p. 782–789.
[80] Holmgren, Å., *Vulnerability analysis of electric power delivery networks*. 2004, Mark och vatten.
[81] Haimes YY. On the definition of vulnerabilities in measuring risks to infrastructures. Risk Analysis 2006;26(2):293–6.
[82] Vereinte Nationen and Int Strategy for Disaster Reduction. Living with risk - a global review of disaster reduction initiatives. 2004 ed. New York; Geneva: United Nations; 2004. 2 Bd.
[83] Johansson J, Hassel H, Zio E. Reliab and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems. Reliab Eng Syst Saf 2013;120:27–38.
[84] Baldick R, et al. Vulnerability assessment for cascading failures in electric power systems. Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES. 2009.
[85] Ouyang M, et al. Comparisons of complex network based models and direct current power flow model to analyze power grid vulnerability under intentional attacks. Physica a-Statistical Mechanics Appl 2014;403:45–53.
[86] NERC, *Security guidelines for the electricity sector: Vulnerability and risk assessment.* Technical Report, Washington, DC, North American Electric Reliab Corporation., 2002.
[87] Vamanu, B.I., A.V. Gheorghe, and P.F. Katina, *Critical Infrastructures: Risk and Vulnerability Assessment in Transportation of Dangerous Goods Transportation by Road and Rail*, in Topics in Safety, Risk, reliability and quality,. Springer.
[88] Dwivedi A, Yu XH. A Maximum-Flow-Based Complex Network Approach for Power System Vulnerability Analysis. IEEE Trans Industr Inform 2013;9(1):81–8.
[89] Gao JX, Barzel B, Barabasi AL. Universal resilience patterns in complex networks. Nature 2016;530(7590):307–12.
[90] Hosseini S, Barker K, Ramirez-Marquez JE. A review of definitions and measures of system resilience. Reliab Eng Syst Saf 2016;145:47–61.
[91] 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.
[92] Bompard, E., D. Wu, and E. Pons, *Complex Sci Application to the Analysis Power Syst Vulnerabilities*.
[93] Rosas-Casals M, Valverde S, SolÉ RV. Topological vulnerability of the european power grid under errors and attacks. Int J Bifurcation Chaos 2007;17(07):2465–75.
[94] Helber S. Performance analysis of flow lines with non-linear flow of material. Berlin; New York: Spinger; 1999.
[95] Tuffin B, et al. *Simulation* versus *analytic-numeric methods: illustrative examples*. Proceedings of the 2nd international conference on Performance evaluation methodologies and tools. Nantes, France: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering); 2007. p. 1–10.
[96] Billinton R, Li W. Reliab assessment of electric power systems using Monte Carlo methods. The language science xvi. New York: Plenum Press; 1994. p. 351.
[97] Liu G-Y, Liu C, Wang Y. Montecarlo simulation for the seismic response analysis of electric power system in Taiwan. NCREE/JRC joint workshop. Citeseer; 2003.
[98] Boccaletti S, et al. Complex networks: Structure and dynamics. Physics Reports 2006;424(4):175–308.
[99] Rosas-Casals M, et al. Knowing power grids and understanding complexity science. Int J Critical Infrastruct 2015;11(1):4–14.
[100] Dorogovtsev, S.N. and J.F.F. Mendes, *Evolution of Networks: From Biological Nets to the Internet and WWW*. 2003.
[101] Ouyang M, et al. Comparisons of complex network based models and real train flow model to analyze Chinese railway vulnerability. Reliab Eng Syst Safety 2014;123:38–46.
[102] Zhang J, et al. Structural vulnerability and intervention of high speed railway networks. Physica A: Statistical Mechanics Appl 2016;462:743–51.
[103] Haznagy A, et al. Complex network analysis of public transportation networks: A comprehensive study. Int Conference onModels and Technologies for Intelligent Transportation Systems (MT-ITS), 2015. 2015.
[104] Dehghani MS, Sherali HD. A resource allocation approach for managing critical network-based infrastructure systems. Iie Trans 2016;48(9):826–37.
[105] Hossain MM, Alam S. A complex network approach towards modeling and analysis of the Australian Airport Network. J Air Transp Manage 2017;60:1–9.
[106] Bagler G. Analysis of the airport network of India as a complex weighted network. Physica A: Statistical Mechanics Appl 2008;387(12):2972–80.
[107] Khakzad N, Reniers G. Using graph theory to analyze the vulnerability of process plants in the context of cascading effects. Reliab Eng Syst Saf 2015;143:63–73.
[108] Yong S, et al. Using complex network theory in the Internet engineering. Computer Science & Education (ICCSE), 2012 7th Int Conference on. 2012.
[109] Thai MT, Pardalos PM. Handbook of optimization in complex networks: communication and social networks. Springer optimization and its applications xii. Gainesville, FL: Springer; 2012. p. 541.
[110] Thai MT, Pardalos PM. Handbook of optimization in complex networks: theory and applications. Springer optimization and its applications xiv. New York, NY: Springer; 2012. p. 544.
[111] De Meo P, et al. A novel measure of edge centrality in social networks. Knowledge-Based Syst 2012;30:136–50.
[112] Costa LdF, et al. Analyzing and modeling real-world phenomena with complex networks: a survey of applications. Adv Physics 2011;60(3):329–412.
[113] Guimera R, Amaral LAN. Functional cartography of complex metabolic networks. Nature 2005;433(7028):895–900.
[114] Barrat A, Barthelemy M, Vespignani A. Dynamical processes on complex networks. Cambridge: Cambridge University Press; 2008.
[115] Freeman LC, Borgatti SP, White DR. Centrality in Valued Graphs - a Measure of Betweenness Based on Network Flow. Social Networks 1991;13(2):141–54.
[116] Nasiruzzaman ABM, Pota HR, Islam FR. Complex network framework based dependency matrix of electric power grid. Universities Power Engineering Conference (AUPEC), 2011 21st Australasian. 2011.
[117] Fang Y, Zio E. Hierarchical Modeling by Recursive Unsupervised Spectral Clustering and Network Extended Importance Measures to Analyze the Reliab Characteristics of Complex Network Systems. Am J Oper Res 2013;3:12.
[118] Sánchez JEC. A complex network approach to analyzing the structure and dynamics of power grids. The University of Vermont; 2009.
[119] Ben-Naim E, Frauenfelder H, Toroczkai Z. Complex networks. Berlin; [Great Britain]: Springer; 2004.
[120] Newman MEJ. Networks: an introduction. Oxford: Oxford University Press; 2010.
[121] Estrada E. The structure of complex networks: theory and applications. New York: Oxford University Press; 2012.
[122] Schneider CM. The robustness of complex networks. , Technische Universität Dortmund; 2011.
[123] Ayyub BM. Vulnerability, uncertainty, and risk: analysis, modeling and management. Reston, Va.: American Soc of Civil Engineers; 2011.
[124] Costa LD, et al. Characterization of complex networks: A survey of measurements. Adv Phys 2007;56(1):167–242.
[125] Bompard E, Napoli R, Xue F. Analysis of structural vulnerabilities in power transmission grids. Int J Critical Infrastruct Prot 2009;2(1-2):5–12.
[126] *Power system test case archive*. Available from: https://www2.ee.washington.edu/research/pstca/pf14/pg_tca14bus.htm.
[127] Bastian, M., S. Heymann, and M. Jacomy, *Gephi: An Open Source Software for Exploring and Manipulating Networks*. 2009. 2009.
[128] Newman MEJ. A measure of betweenness centrality based on random walks. Social Netw 2005;27(1):39–54.
[129] Latora V, Marchiori M. A measure of centrality based on network efficiency. New J Phys 2007;9(6):188.
[130] Guan X, et al. Power grids vulnerability analysis based on combination of degree and betweenness. The 26th Chinese Control and Decision Conference (2014 CCDC). 2014.
[131] Newman MEJ. The Structure and Function of Complex Networks. SIAM Rev 2003;45(2):167–256.
[132] Bai Wj, et al. Electric Power Grids and Blackouts in Perspective of Complex Networks. 2006 Int Conference on Communications, Circuits and Systems. 2006.
[133] Klopotek MA, Wierzchon ST, Trojanowski K. Intelligent Information Processing and Web Mining. Proceedings of the Int IIS: IIPWḾ 06 Conference held in Ustron, Poland, June 19-22, 2006. Berlin Heidelberg: Springer; 2007.
[134] Rosato V, Bologna S, Tiriticco F. Topological properties of high-voltage electrical transmission networks. Electr Power Syst Res 2007;77(2):99–105.
[135] Hines P, Blumsack S. A Centrality Measure for Electrical Networks. Hawaii Int Conference on System Sciences, Proceedings of the 41st Annual. 2008.
[136] Erdos P, Renyi A. On the Evolution of Random Graphs. Bull Int Stati Instit 1960;38(4):343–7.
[137] Watts DJ, Strogatz SH. Collective dynamics of 'small-world' networks. Nature 1998;393(6684):440–2.
[138] Crucitti P, Latora V, Marchiori M. Model for cascading failures in complex networks. Phys Rev E 2004;69(4).
[139] Pagani GA, Aiello M. From the grid to the smart grid, topologically. Physica a-Statl Mech 2016;449:160–75.
[140] Newman MEJ. Analysis of weighted networks. Phys. Rev. E 2004;70(5):056131.
[141] Pagani GA, Aiello M. A complex network approach for identifying vulnerabilities of the medium and low voltage grid. Int J Critical Infrastructs 2015;11(1):36–61.
[142] Zio E, Golea LR. Analyzing the topological, electrical and reliability characteristics of a power transmission system for identifying its critical elements. Reliab Eng Syst Saf 2012;101:67–74.
[143] Liu C, et al. Vulnerability evaluation of power system integrated with large-scale distributed generation based on complex network theory. 2012 47th Int Universities Power Engineering Conference (UPEC). 2012.
[144] Cadini F, Zio E, Petrescu C-A. Using Centrality Measures to Rank the Importance of the Components of a Complex Network Infrastructure. In: Setola R, Geretshuber S, editors. Critical Information Infrastructure Security: Third Int Workshop, CRITIS 2008, Rome, Italy, October13-15, 2008. Revised Papers. Berlin, Heidelberg: Springer Berlin Heidelberg; 2009. p. 155–67.
[145] Nasiruzzaman ABM, Pota HR, Mahmud MA. Application of centrality measures of complex network framework in power grid. IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Soc. 2011.
[146] Arianos S, et al. Power grid vulnerability: A complex network approach. Chaos 2009;19(1).
[147] Crucitti P, Latora V, Marchiori M. Locating critical lines in high-voltage electrical power grids. Fluctuation Noise Letters 2005;5(2):L201–8.
[148] Holmgren AJ. Using graph models to analyze the vulnerability of electric power

networks. Risk Analysis 2006;26(4):955–69.
[149] Chen X, et al. Identification of Vulnerable Lines in Power Grid Based on Complex Network Theory. 2007 IEEE Power Engineering Soc General Meeting. 2007.
[150] Zio E, Petrescu C-A, Sansavini G. Vulnerability analysis of a power transmission system. Proc. Int Probabilistic Safety Assessment and Management Conference (PSAM). 2008.
[151] Buzna L, Issacharoff L, Helbing D. The evolution of the topology of high-voltage electricity networks. Int J Critical Infrastruct 2009;5(1-2):72–85.
[152] 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.
[153] Chen G, et al. An improved model for structural vulnerability analysis of power networks. Physica A-Statistical Mechanics Appl 2009;388(19):4259–66.
[154] Zio E, Piccinelli R. Randomized flow model and centrality measure for electrical power transmission network analysis. Reliab Eng Syst Saf 2010;95(4):379–85.
[155] Bompard E, Wu D, Xue F. The Concept of Betweenness in the Analysis of Power Grid Vulnerability. Complexity in Eng, 2010. COMPENG '10 2010.
[156] Jin S, et al. A novel application of parallel betweenness centrality to power grid contingency analysis. 2010 IEEE Int Symposium on Parallel & Distributed Processing (IPDPS). 2010.
[157] Wang Z, Scaglione A, Thomas RJ. Electrical centrality measures for electric power grid vulnerability analysis. 49th IEEE Conference on Decision and Control (CDC). 2010.
[158] Fu L, et al. Vulnerability Assessment for Power Grid Based on Small-world Topological Model. 2010 Asia-Pacific Power and Energy Engineering Conference. 2010.
[159] Hines P, Cotilla-Sanchez E, Blumsack S. Do topological models provide good information about electricity infrastructure vulnerability? Chaos 2010;20(3).
[160] Zhang JH, et al. Attack vulnerability of self-organizing networks. Safety Sci 2012;50(3):443–7.
[161] Bompard E, Napoli R, Xue F. Extended topological approach for the assessment of structural vulnerability in transmission networks. Iet Generation Transm Distribution 2010;4(6):716–24.
[162] Wang K, et al. An electrical betweenness approach for vulnerability assessment of power grids considering the capacity of generators and load. Physica A-Stat Mech Appl 2011;390(23-24):4692–701.
[163] Wu Zg, Zhong Q, Zhang Y. State Transition Graph of Cascading Electrical Power Grids. 2007 IEEE Power Engineering Soc General Meeting. 2007.
[164] Bompard E, Wu D, Xue F. Structural vulnerability of power systems: A topological approach. Electr Power Syst Res 2011;81(7):1334–40.
[165] Zio, E., et al., *Application of the load flow and random flow models for the analysis of power transmission networks*. Reliab Engineering & System Safety, 2012. 103: p. 102–109.
[166] Bompard E, Pons E, Wu D. Extended Topological Metrics for the Analysis of Power Grid Vulnerability. Ieee Syst J 2012;6(3):481–7.
[167] Kong R, et al. An Energy-Based Centrality for Electrical Networks. Energy Power Eng 2013;5:6.
[168] Huang X, et al. Vulnerability Analysis of Bus Failure in Power Grid. Third Int Conference on Control, Automation and Systems Engineering (CASE-13). Citeseer; 2013.
[169] Zhang GD, et al. Understanding the cascading failures in Indian power grids with complex networks theory. Physica a 2013;392(15):3273–80.
[170] Alipour MASMaZ. Structural Properties and vulnerability of Iranian 400kv Power Transmission Grid: a Complex Systems Approach. Industrial Eng Manage 2013.
[171] Kim DH, et al. Network topology and resilience analysis of South Korean power grid. Physica a- 2017;465:13–24.
[172] Ouyang M, et al. Correlation analysis of different vulnerability metrics on power grids. Physica a 2014;396:204–11.
[173] Xu Y, Gurfinkel AJ, Rikvold PA. Architecture of the Florida power grid as a complex network. Physica a 2014;401:130–40.
[174] Zhu Y, et al. Revealing Cascading Failure Vulnerability in Power Grids Using Risk-Graph. IEEE Trans Parallel Distributed Syst 2014;25(12):3274–84.
[175] Li C, et al. Method for evaluating the importance of power grid nodes based on PageRank algorithm. IET Gen, Trans Distribut 2014;8:1843–7.
[176] Zhang JH, et al. Vulnerability analysis of the US power grid based on local load-redistribution. Safety Sci 2015;80:156–62.
[177] Coelho EP, et al. A complex network analysis of the brazilian power test System. in innovative smart grid technologies latin america (ISGT LATAM), 2015 IEEE PES. IEEE; 2015.
[178] Chowdhury T, Chakrabarti A, Chanda CK. Analysis of Vulnerability indices of power grid integrated DG units based on Complex Network theory. India Conference (INDICON), 2015 Annual IEEE. IEEE; 2015.
[179] WANG H, et al. Evaluation method of node importance for power grid considering inflow and outflow power. J Modern Power Syst Clean Energy 2017;5(5):696–703.
[180] Albarakati A, Bikdash M, Dai X. Line-graph based modeling for assessing the vulnerability of transmission lines. SoutheastCon, 2017. IEEE; 2017.
[181] Dey, A.K., Y.R. Gel, and H.V. Poor, *Motif-based analysis of power grid robustness under attacks*. arXiv preprint arXiv:1708.06738, 2017.
[182] Wang SL, et al. Vulnerability analysis and critical areas identification of the power systems under terrorist attacks. Physica a 2017;473:156–65.
[183] Gupta S, et al. Analysis and prediction of vulnerability in smart power transmission system: A geometrical approach. Int J Electr Power Energy Syst 2018;94:77–87.
[184] Wang ZY, et al. A power flow based model for the analysis of vulnerability in power networks. Physica a 2016;460:105–15.
[185] Yuan Y, et al. Probabilistic load flow computation of a power system containing wind farms using the method of combined cumulants and Gram-Charlier expansion. Iet Renewable Power Generation 2011;5(6):448–54.
[186] Kundur P, Balu NJ, Lauby MG. Power system stability and control. The EPRI power system engineering series xxiii. New York: McGraw-Hill; 1994. p. 1176.
[187] Stevenson WD. Elements of power system analysis. 4th ed. Mcgraw-hill series in electrical engineering power and energy xii. New York: McGraw-Hill; 1982. p. 436.
[188] Saadat H. Power system analysis. McGraw-Hill series in electrical and computer engineering xix. Boston: WCB/McGraw-Hill; 1999. p. 697.
[189] LaRocca S, et al. Topological performance measures as surrogates for physical flow models for risk and vulnerability analysis for electric power systems. Risk Anal 2015;35(4):608–23.
[190] Yan J, et al. Cascading Failure Analysis With DC Power Flow Model and Transient Stability Analysis. IEEE Trans Power Syst 2015;30(1):285–97.
[191] Carreras BA, et al. Dynamical and probabilistic approaches to the study of blackout vulnerability of the power transmission grid. 37th Annual Hawaii Int Conference on System Sciences, 2004. Proceedings of the. 2004.
[192] Nedic DP, et al. Criticality in a cascading failure blackout model. Int J Electr Power Energy Syst 2006;28(9):627–33.
[193] Dobson I, Carreras BA, Newman DE. A loading-dependent model of probabilistic cascading failure. Probab Eng Informational Scis 2005;19(1):15–32.
[194] Cupac V, Lizier JT, Prokopenko M. Comparing dynamics of cascading failures between network-centric and power flow models. Int J Electr Power Energy Syst 2013;49:369–79.
[195] Fitzmaurice, R., *Cascading Failure in a Complex System Model for Power Systems: Operating and Planning Policy*. 2010: University College Dublin.
[196] Han SW, Peng ZX, Wang SQ. The maximum flow problem of uncertain network. Inf Sci 2014;265:167–75.
[197] Fan WL, Huang SW, Mei SW. Invulnerability of power grids based on maximum flow theory. Physica a-Statistical Mechanics Appl 2016;462:977–85.
[198] Fang J, et al. Power System Structural Vulnerability Assessment based on an Improved Maximum Flow Approach. IEEE Trans Smart Grid 2016(99):1. 1.
[199] Zhang P, Lee ST. Probabilistic load flow computation using the method of combined cumulants and Gram-Charlier expansion. IEEE Trans Power Syst 2004;19(1):676–82.
[200] Marah B, Ekwue AO. Probabilistic load flows. Power Engineering Conference (UPEC), 2015 50th Int Universities. 2015.
[201] Ma J, et al. Probabilistic vulnerability assessment based on power flow and voltage distribution. IEEE PES T&D 2010 2010.
[202] Wang XF, Song Y, Irving M. Modern power systems analysis. US: Springer; 2010.
[203] Ran XH, Miao SH. Three-phase probabilistic load flow for power system with correlated wind, photovoltaic and load. Iet Generation Transmission Distribution 2016;10(12):3093–101.
[204] Dwivedi A, Yu X, Sokolowski P. Analyzing power network vulnerability with maximum flow based centrality approach. 2010 8th IEEE Int Conference on Industrial Informatics. 2010.
[205] Nasiruzzaman ABM, Pota HR. Critical node identification of smart power system using complex network framework based centrality approach. North American Power Symposium (NAPS), 2011. 2011.
[206] Wang J, et al. Identifying line vulnerability in power system using maximum flow based complex network theory. IECON 2014 - 40th Annual Conference of the IEEE Industrial Electronics Soc. 2014.
[207] Dai Y, et al. An improved framework for power grid vulnerability analysis considering critical system features. Physica A: Stat Mech Appl 2014;395:405–15.
[208] Singh, A.K. and B.C. Pal, *IEEE PES Task Force on Benchmark Systems for Stability Controls Report on the 68-Bus, 16-Machine, 5-Area System*. 2013, Technical Report.
[209] Correa GJ, Yusta JM. *Grid vulnerability analysis based on scale-free graphs* versus *power flow models*. Electr Power Syst Res 2013;101:71–9.
[210] Correa-Henao GJ, Yusta-Loyo JM. Representation of electric power systems by complex networks with applications to risk vulnerability assessment. Dyna 2015;82(192):68–77.
[211] Kim, T., et al., *Vulnerability analysis of power systems*. arXiv preprint arXiv:1503.02360, 2015.
[212] Wang X, et al. A network approach for power grid robustness against cascading failures. 2015 7th Int Workshop on Reliable Networks Design and Modeling (RNDM). 2015.
[213] da Silva AML, et al. A Method for Ranking Critical Nodes in Power Networks Including Load Uncertainties. IEEE Trans Power Syst 2016;31(2):1341–9.
[214] Grigg C, et al. The IEEE Reliab Test System-1996. A report prepared by the Reliab Test System Task Force of the Application of Probability Methods Subcommittee. IEEE Trans Power Syst 1999;14(3):1010–20.
[215] Werho T, et al. Power System Connectivity Monitoring Using a Graph Theory Network Flow Algorithm. IEEE Trans Power Syst 2016(99):1–8.
[216] Li J, et al. AC power flow importance measures considering multi-element failures. Reliab Eng Syst Saf 2017;160:89–97.
[217] Fang R, et al. Identification of vulnerable lines in power grids with wind power integration based on a weighted entropy analysis method. Int J Hydrogen Energy 2017;42(31):20269–76.
[218] Liu B, et al. Recognition and Vulnerability Analysis of Key Nodes in Power Grid Based on Complex Network Centrality. IEEE Trans Circuits Syst II: Express Briefs 2017.
[219] Von Neumann J, Morgenstern O. Theory of games and economic behavior. 3d ed. Princeton: Princeton University Press; 1953. p. 641.
[220] Bompard E, et al. Risk Assessment of Malicious Attacks Against Power Syst. IEEE Trans Syst Man Cybern Part a-Systems Humans 2009;39(5):1074–85.
[221] Cheng MX, Crow M, Ye QM. A game theory approach to vulnerability analysis: Integrating power flows with topological analysis. Int J Electr Power Energy Syst 2016;82:29–36.
[222] Wang, Q., *Game Theory Approach to Transportation Network Vulnerability Measurement*. 2012.
[223] Bricha N, Nourelfath M. Critical supply network protection against intentional attacks: A game-theoretical model. Reliab Eng Syst Saf 2013;119:1–10.
[224] Flammini F. Critical infrastructure security: assessment, prevention, detection, response. Inf Commun Technol 2012:303.

[225] Matsumoto A, Szidarovszky F. Game theory and its applications. Institute of economic research xiv. Toyko; New York: Springer; 2016. p. 268.
[226] Holmgren AJ, Jenelius E, Westin J. Evaluating strategies for defending electric power networks against antagonistic attacks. IEEE Trans Power Syst 2007;22(1):76–84.
[227] Korzhyk D, et al. *Stackelberg* vs. *Nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness*. J Artificial Intell Res 2011;41:297–327.
[228] Sinha A, et al. Stackelberg Security Games: Looking Beyond a Decade of Success. IJCAI 2018.
[229] Gomez C, et al. Hierarchical infrastructure network representation methods for risk-based decision-making. Struct Infrastruct Eng 2013;9(3):260–74.
[230] Agarwal J, Blockley D, Woodman N. Vulnerability of structural systems. Struct Saf 2003;25(3):263–86.
[231] Cortes JAMB, Sanchez-Silva M, Tesfamariam S. A hierarchy- based approach to seismic vulnerability assessment of bulk power systems. Structure Infrastruct Eng 2015;11(10):1352–68.
[232] Gómez C, et al. Vulnerability assessment of infrastructure networks by using hierarchical decomposition methods. Vulner, Uncertainty, Risk 2011:214–21.
[233] Ruan D. Fuzzy systems and soft computing in nuclear engineering. Heidelberg: Physica Verlag; 2000.
[234] Schaeffer SE. Graph clustering. Comput Sci Rev 2007;1(1):27–64.
[235] Wang A, et al. Vulnerability Assessment Scheme for Power System Transmission Networks Based on the Fault Chain Theory. IEEE Trans Power Syst 2011;26(1):442–50.
[236] Zhang C, Ramirez-Marquez JE, Wang JH. Critical infrastructure protection using secrecy - A discrete simultaneous game. Euro J Oper Res 2015;242(1):212–21.
[237] Zechman EM. Agent-based modeling to simulate contamination events and evaluate threat management strategies in water distribution systems. Risk Anal 2011;31(5):758–72.
[238] Gonzalez de Durana JM, et al. Agent based modeling of energy networks. Energy Conver Manage 2014;82:308–19.
[239] Stroeve SH, Everdij MHC. Agent-based modelling and mental simulation for resilience engineering in air transport. Saf Sci 2017;93:29–49.
[240] Ali AM, Shafiee ME, Berglund EZ. Agent-based modeling to simulate the dynamics of urban water supply: Climate, population growth, and water shortages. Sust Cities Soc 2017;28:420–34.
[241] Galus, M.D., *Agent-based modeling and simulation of large scale electric mobility in power systems*. 2012, s.n.,: S.l. p. XX, 294 S.
[242] Sujil A, Verma J, Kumar R. Multi agent system: concepts, platforms and applications in power systems. Artif Intell Rev 2016.
[243] Dehghanpour K, Colson C, Nehrir H. A Survey on Smart Agent-Based Microgrids for Resilient/Self-Healing Grids. Energies 2017;10(5):620.
[244] Xie J, Liu C-C. Multi-agent systems and their applications. J Int Council Electr Eng 2017;7(1):188–97.
[245] Akyol, B., et al., *VOLTTRON: An Agent Execution Platform for the Electric Power System*. 2017.
[246] Yan H, et al. Branch transient vulnerability assessment based on the transient energy function and complex network. 2014 Int Conference on Power System Technology. 2014.
[247] Jurado F, Carpio J. Energy functions analysis in voltage collapse. Eur Trans Electr Power 2001;11(4):235–40.
[248] Pai MA. Energy function analysis for power system stability. The kluwer international series in engineering and computer science power electronics and power systems viii. Boston: Kluwer Academic Publishers; 1989. p. 240.
[249] Tsolas NA, Arapostathis A, Varaiya PP. A Structure Preserving Energy Function for Power-System Transient Stability Analysis. IEEE Trans Circuits Syst 1985;32(10):1041–9.
[250] Chow JH, et al. Synchronized phasor data based energy function analysis of dominant power transfer paths in large power systems. IEEE Trans Power Syst 2007;22(2):727–34.
[251] Bhui P, Senroy N. Real-Time Prediction and Control of Transient Stability Using Transient Energy Function. IEEE Trans Power Syst 2017;32(2):923–34.
[252] Fouad AA, Qin Z, Vittal V. System vulnerability as a concept to assess power system dynamic security. IEEE Trans Power Syst 1994;9(2):1009–15.
[253] Padiyar KR, Sastry HSY. Topological energy-function analysis of stability of power systems. Int J Electr Power Energy Syst 1987;9(1):9–16.
[254] Rangaiah GP. Multi-objective optimization: techniques and applications in chemical engineering, in advances in process systems engineering. Singapore: World Scientific Publishing; 2017.
[255] Cho JH, et al. A Survey on Modeling and Optimizing Multi-Objective Systems. IEEE Commun Surveys Tutorials 2017;19(3):1867–901.
[256] Babick JP. Tri-level optimization of critical infrastructure resilience. Monterey, California: Naval Postgraduate School; 2009.
[257] Faramondi L, et al. Network Structural Vulnerability: A Multiobjective Attacker Perspective. IEEE Trans Syst, Man, Cybernetics: Syst 2018(99):1–14.
[258] Mingoo K, El-Sharkawi MA, Marks RJ. Vulnerability indices for power systems. Proceedings of the 13th Int Conference on, Intelligent Systems Application to Power Systems. 2005.
[259] Haidar AMA, Mohamed A, Hussain A. Vulnerability Assessment of a Large Sized Power System Using Radial Basis Function Neural Network. 2007 5th Student Conference on Research and Development. 2007.
[260] Pinar A, Reichert A, Lesieutre B. Computing Criticality of Lines in Power Systems. 2007 IEEE Int Symposium on Circuits and Systems. 2007.
[261] Jingling L, QunXing J, YongLi Z. Power grid vulnerability assement based on energy function. 2008 Third Int Conference on Electric Utility Deregulation and Restructuring and Power Technologies. 2008.
[262] Liu Q, Liu J, Huang Q. Configure vulnerability assessment based on potential energy model. 2009 Int Conference on Sustainable Power Generation and Supply. 2009.
[263] Dong X, et al. Vulnerability analysis of power grid based on multi-agent complex systems. Proceedings of 2011 IEEE Int Conference on Service Operations, Logistics and Informatics. 2011.
[264] Huang Zm, Li Hq. Vulnerable Branch Assessment Based on Branch Energy Function. 2012 Asia-Pacific Power and Energy Engineering Conference. 2012.
[265] Witthaut D, et al. Critical Links and Nonlocal Rerouting in Complex Supply Networks. Phys Rev Lett 2016;116(13):138701.
[266] Kröger W, Zio E, Schläpfer M. Vulnerable systems xiv. London: Springer; 2011. p. 204.
[267] Corder GW, Foreman DI. Nonparametric statistics for non-statisticians: a step-by-step approach. Oxford: Wiley-Blackwell; 2009.
[268] Zio, E., C.-A. Petrescu, and G. Sansavini. *Vulnerability analysis of a power transmission system*.
[269] Rocchetta R, Patelli E. Assessment of power grid vulnerabilities accounting for stochastic loads and model imprecision. Int J Electr Power Energy Syst 2018;98:219–32.
[270] Cadini F, Agliardi GL, Zio E. A modeling and simulation framework for the reliability/availability assessment of a power transmission grid subject to cascading failures under extreme weather conditions. Applied Energy 2017;185(Part 1):267–79.
[271] Baldick R, et al. Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding, prediction, mitigation and restoration of cascading failures. 2008 IEEE Power and Energy Soc General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century. 2008.
[272] Rosato V, et al. Modelling interdependent infrastructures using interacting dynamical models. Int J Critical Infrastruct 2008;4(1-2):63–79.
[273] Arghandeh R, et al. On the definition of cyber-physical resilience in power systems. Renewable Sust Energy Rev 2016;58:1060–9.
[274] Nezamoddini N, Mousavian S, Erol-Kantarci M. A risk optimization model for enhanced power grid resilience against physical attacks. Electr Power Syst Research 2017;143(Supplement C):329–38.
[275] Ma T-L, et al. Non-monotonic increase of robustness with capacity tolerance in power grids. Physica A 2013;392(21):5516–24.
[276] Schneider CM, et al. Mitigation of malicious attacks on networks. Proc Natl Acad Sci United States America 2011;108(10):3838–41.
[277] Pagani GA, Aiello M. Power grid complex network evolutions for the smart grid. Physica a-Statistical Mechanics Appl 2014;396:248–66.
[278] Bompard E, et al. Classification and trend analysis of threats origins to the security of power systems. Int J Electr Power Energy Syst 2013;50(Supplement C):50–64.
[279] Chu C-C, Iu HH-C. Complex Networks Theory For Modern Smart Grid Applications: A Survey. IEEE J Emerg Select Topics Circuits Syst 2017.
[280] Wang CW, Grebogi C, Baptista MS. Control and prediction for blackouts caused by frequency collapse in smart grids. Chaos 2016;26(9).
[281] Wang W, Lu Z. Survey Cyber security in the Smart Grid: Survey and challenges. Comput. Netw. 2013;57(5):1344–71.
[282] Gao J, et al. Recent Progress on the Resilience of Complex Networks. Energies 2015;8(10):12187.
[283] Heitzig J, et al. Interdisciplinary challenges in the study of power grid resilience and stability and their relation to extreme weather events. European Phys J-Special Topics 2014;223(12):2383–6.
[284] Strbac G, et al. Microgrids: Enhancing the Resilience of the European Megagrid. IEEE Power Energy Mag 2015;13(3):35–43.
[285] Zio E. Critical Infrastructures Vulnerability and Risk Analysis. Eur J Security Res 2016;1(2):97–114.
[286] Huang T, et al. The Structural Dimensions in the Security of Power Transmission Systems. In: Gheorghe AV, Masera M, Katina PF, editors. Infranomics 2014:311–37.
[287] Gheorghe AV, Katina PF, Masera M. Infranomics: sustainability, engineering design and governance. Cham: Springer; 2014.