Reliability Engineering and System Safety 196 (2020) 106788

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

A comprehensive framework for vulnerability analysis of extraordinary events in power systems

Iver Bakken Sperstad*, Gerd H. Kjølle, Oddbjørn Gjerde

SINTEF Energy Research, P.O. Box 4761 Torgarden, NO-7465, Trondheim, Norway

ARTICLE INFO

Keywords:
Power system vulnerability
Resilience engineering
Risk analysis
Robustness
High-impact low-probability events
Extreme events

ABSTRACT

Electric power systems are critical infrastructures subject to the possibility of extraordinary events with high societal consequences. Although such possibilities are often associated with very low probabilities of being realized, it is nevertheless crucial to be able to identify and understand the vulnerabilities of power systems related to extraordinary events. The objective of the work presented in this article is to establish a methodological basis for vulnerability analysis that is complementary to conventional risk and reliability analysis of power systems. It presents a comprehensive framework of definitions, indicators and methods that can be used to classify, analyse and monitor vulnerabilities in power transmission and distribution systems. Its main components include (1) a conceptual framework of definitions that forms the basis for understanding and classifying vulnerabilities, (2) an assessment methodology for identifying vulnerabilities related to extraordinary events and barriers to mitigate them, and (3) vulnerability indicators for quantifying and monitoring power system vulnerabilities. The applicability of the vulnerability analysis framework is demonstrated through several studies of real power systems. Moreover, the concept of power system vulnerability elaborated in this article is also related to the concept of power system resilience.

1. Introduction

Society is increasingly dependent on a secure electricity supply to maintain its functionality and cover basic needs. As a consequence, a secure electricity supply is *critical* for the society, and the electric power system is thus one of society's critical infrastructures [1], defined as physical and logical systems essential for social welfare [2,3]. The essential role of electricity is perhaps most evident at the rare occurrences of extensive and/or long-lasting interruptions of electricity supply, i.e. *blackout* events [4]. Such events result in large direct and indirect economic consequences to the end-users of the power system [5,6], and the dependence of other critical infrastructures on the power system may in addition lead to indirect societal costs that are just as large or larger [7,8]. Moreover, it has been argued that repeated occurrences of blackout events during the past few decades and the emergence of new threats indicate that power systems are becoming increasingly vulnerable [9].

Motivated by the vital role of the electric power system and the crucial need to better understand the vulnerabilities of power systems, the objective of the work presented in this article is to establish a methodological basis for analysing vulnerabilities related to extraordinary events in power systems. We will use the more general term *extraordinary events* to denote events such as blackout events that have high societal consequences and are associated with low probabilities of occurring (often referred to as HILP events or extreme events). This term is used to distinguish them from the “ordinary” events encountered in daily system operation and conventional power system reliability and risk analysis.

Although extraordinary events may be associated with a low level of risk, due to a low estimated probability of occurrence according to conventional risk analysis [5,10], the level of criticality of the consequences may nevertheless make it unacceptable to the stakeholders to neglect them [11]. The analysis of extraordinary events requires approaches that are distinct and complementary to the risk and reliability analysis approaches appropriate for more frequent events, and broader frameworks are needed to better understand and communicate about the risks associated with extraordinary events [1,12,13]. Therefore, considerable attention within the field of power system analysis has recently been given to concepts and perspectives such as vulnerability, resilience and robustness [5,14–18]. For instance, modelling frameworks based on extended risk concepts also considering extraordinary events are described in [19,20,21], a framework for developing resilience metrics is described in [22], and a resilience assessment methodology for extreme weather events is presented in [23]. According to

* Corresponding author.
E-mail address: iver.bakken.sperstad@sintef.no (I.B. Sperstad).

https://doi.org/10.1016/j.ress.2019.106788
Received 17 June 2019; Received in revised form 13 November 2019; Accepted 28 December 2019
Available online 30 December 2019

the literature, one may distinguish between analysis of blackout events due to natural hazards and other blackout events (e.g. cascading blackouts due to random failures or intentional attacks) [5]. Methods considering natural hazards are reviewed in e.g. [24,25], and methods for analysing cascading events are reviewed in e.g. [26,27], respectively.

In this article, we do not limit ourselves to any specific type of extraordinary event but consider the perspective of power system vulnerability in a broader sense, as elaborated below. The article describes a comprehensive framework of definitions, indicators and methods that can be used to classify, analyse and monitor vulnerabilities in power transmission and distribution systems relevant for extraordinary events and applicable for both planning and operation purposes [28,29]. This framework has been developed and thoroughly tested on real power systems over a number of years. These developments built upon a methodology for analysing the vulnerability of power systems that was previously presented in [11]. Historic extraordinary events are analysed in [30,31]. The framework and the development of vulnerability indicators were later presented in [32–34,29], while a novel vulnerability assessment methodology was introduced in [35]. Furthermore, the vulnerability analysis framework presented in this article forms the basis for the risk analysis approach underlying the European research projects GARPUR [36] and AFTER [21].

A main contribution of the present article is to give a complete and unified description of the vulnerability analysis framework and its constituent methodologies. Secondly, we demonstrate and summarize the application of the vulnerability analysis framework to a variety of real power system cases. Whereas most existing approaches to power system vulnerability analysis implement specific methods and models [5], we propose a more general and comprehensive approach in which different qualitative and quantitative methods can be incorporated, depending on the case. The approach is designed specifically for power systems, and we argue and exemplify how the physics of the power system must be considered when applying the framework and selecting which methods to implement [1,5,37].

In Section 2, we first elaborate on the concept of extraordinary events in power systems. Then, in the following sections, the main components of the vulnerability analysis are presented: Section 3 introduces the overarching conceptual vulnerability framework and establishes a nomenclature for classifying and understanding power system vulnerability, including its relationship with power system resilience. On this basis, a general methodology for vulnerability assessment is presented in Section 4 and the development of vulnerability indicators for quantifying different aspects of vulnerability is presented in Section 5. The application of the methodologies is demonstrated and exemplified in Section 6, where a selection of studies of power systems are summarized, before the article is concluded in Section 7.

2. Extraordinary events in power systems

To illustrate the concept of extraordinary events in power systems, examples of historic events are depicted in a two-dimensional consequence diagram in the upper part of Fig. 1. Here, the consequences are measured in terms of total end-user power interrupted (MW) and interruption duration (hours). Although the criticality of the consequences depends on several other factors to be discussed in more detail below, the two dimensions in Fig. 1 are useful for characterizing broadly the consequences of extraordinary events. In general, events with a) extraordinarily high magnitude of the power interrupted such as the blackouts of Italy and Sweden/Denmark in 2003 [38] or b) extraordinarily long interruption durations such as the storm Gudrun in South-Sweden in 2005 [39] can both be regarded as extraordinary events. Thus, also the local event in Fig. 1 (Steigen, Norway, 2007 [32]) is regarded as an extraordinary event in the proposed framework, since it affected the entire community for six days. Extraordinary events in power systems typically fall into two main categories [5,40]: Events in the first category are primarily due to natural hazards (e.g. major storms) and are characterized by extensive physical damage to the infrastructure and consequently long restoration times and interruption durations [40]. Events in the second category are attributed to more diverse and complex causes, including “random” failures [5] (technical failures [5,40] and operational failures [40] or human errors [41]) as well as intentional/malicious [5,37] attacks. Furthermore, they often involve a multitude of non-technical as well as technical factors, including human and organizational/contextual factors [31,37].

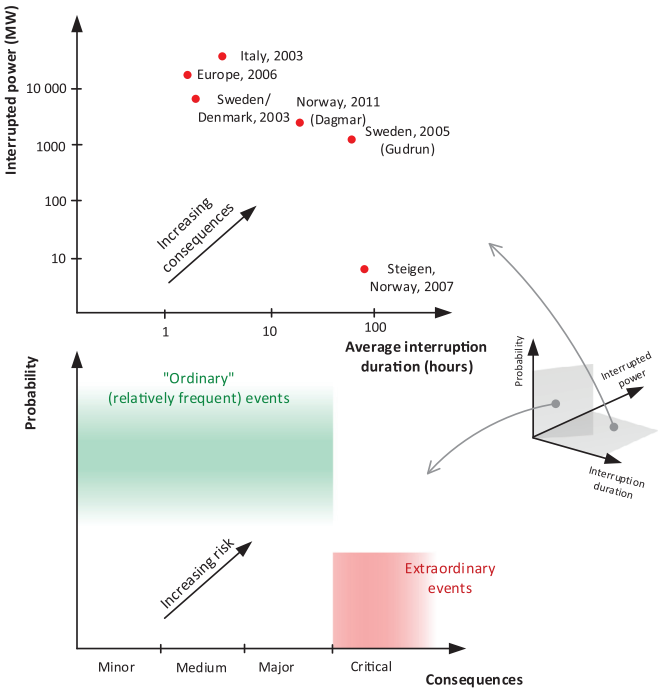

Fig. 1. Schematic consequence diagram (top) and risk diagram (bottom) placing extraordinary power system events in the three-dimensional space spanned by their interrupted power, interruption duration and the estimated probability of their occurrence.

The lower part of Fig. 1 shows a risk diagram where the two dimensions are collapsed into a single consequence dimension for the sake of illustration. Extraordinary events with critical consequences but associated with low probabilities can be found in the lower-right corner. In addition to the two dimensions included in Fig. 1, the criticality depends on and can be characterized by factors such as: size of the affected population/area, time of occurrence, temperature and weather conditions, type of end-users affected, economic consequences, consequences to other infrastructure and society more widely, and consequences for health and life [11,35]. “Critical” is a central term that is assigned a special meaning throughout the proposed framework described in this paper. How severe the consequences must be to be regarded as “critical”, has to be determined by the relevant stakeholders for the particular area under study, i.e. system operators, regulators, and local authorities [11].

3. Power system vulnerability concepts

This section establishes the overarching conceptual framework, the closely associated bow tie model, and the nomenclature that forms the basis for our understanding of power system vulnerability.

3.1. Conceptual framework for power system vulnerability

The term “vulnerability” is in the literature associated with a variety of definitions [5,42]. Based on e.g. [11,43], for the purpose of the proposed framework, we define *vulnerability* as an *expression for the*

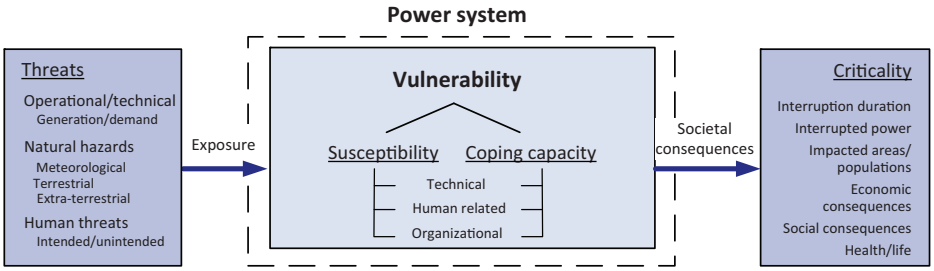

Fig. 2. Illustration of the conceptual vulnerability framework for power systems.

problems a system faces to maintain its function if a threat leads to an unwanted event and the problems the system faces to resume its activities after the event occurred. In the context of power systems, we understand the *unwanted event* to be one or more power system failures, which may lead to interruption of electricity supply. The concept of vulnerability is illustrated in Fig. 2.

The definition of power system vulnerability describes how it is a dualistic concept comprising both the power system's *susceptibility* to threats and its (lack of) *coping capacity* in case of unwanted events: A system is susceptible towards a threat if the threat leads to an unwanted event in the system; the coping capacity describes the ability of the operator and the system itself to cope with an unwanted event, limit negative consequences, and restore the function of the system to a normal state.

Vulnerability is an internal characteristic of the power system, which here includes all technical (e.g., power system components as well as all equipment), human (personnel) and organizational factors of the power system operator. It is nevertheless useful to also consider *dimensions of vulnerability* that are external to the power system: In addition to the internal dimensions (1) susceptibility and (2) coping capacity, the framework depicted in Fig. 2 also comprises the external dimensions of (3) threats and (4) criticality (i.e. to society).

Here we have adopted the definition of a *threat* as any indication, circumstance, or event with the potential to disrupt or destroy a critical infrastructure (here a power system), or any element thereof [2]. We understand a threat as something that in a broad sense exists and develops externally to the power system, and the *exposure* to a threat may cause an unwanted event within the system. Threats may be related to natural hazards, humans or the operational/technical conditions enforced on the system, where the operational conditions include generation and demand imposing operational stress on system components. Ref. [9] gives a more comprehensive discussion of threats relevant to power systems.

The *criticality* dimension refers to the level of criticality of the societal consequences of power system failures. Society is defined as external to the power system, and the term criticality refers to consequences to the end-users and not to the components in the system. This criticality can best be measured by the society's dependence on electricity supply and depends on factors as those described in Section 2.

3.2. Barriers against extraordinary events in power systems

The relationship between the concepts introduced above in relation to vulnerability can be illustrated by the bow tie model shown in Fig. 3. This model structures the causal relationship in sequences of events potentially leading from a threat (left hand side) to an unwanted event (middle) and in turn to societal consequences (right hand side).

We understand an extraordinary event to be a possible sequence of events leading to critical consequences. The unwanted event (power system failures) is related to the concept of a *contingency*, which is understood as a failure or unplanned outage of one or multiple system components [44,45]. In the context of extraordinary events, an unwanted event may be the initiating event of a so-called cascading blackout [4,27,46], or it may be multiple essentially simultaneous failures e.g. due to extreme weather [23,47].

In such sequences of events, a *barrier* is something that either can prevent an event from taking place or protect against its consequences [48]. As depicted in Fig. 3, barriers are associated with either the susceptibility or the coping capacity of the power system, and a vulnerability can be associated with a barrier that is either missing, weak or malfunctioning [30].

Barriers associated with susceptibility on the left-hand side of the bow tie are broadly speaking intended to prevent threats from causing power system failures and thus reduce the probability. These barriers can be associated with actions taken preventively by the system operator. As indicated on the right-hand side of the bow tie model in Fig. 3, barriers exist that may prevent or reduce the societal consequences after the occurrence of power system failures. These barriers can be associated with the coping capacity of the power system, broadly classified in two groups [49]: i) barriers associated with corrective actions (automatic system response and emergency operator actions) with respect to certain power system failures, and ii) barriers associated with the restoration of normal system operation after electricity supply has been interrupted. Broadly speaking, the former barriers are primarily designed to limit the amount of interrupted power and the latter are primarily intended to reduce restoration time and thus the interruption duration. Table 1 shows the proposed classification of power system barriers and a few concrete examples for each group.

3.3. Vulnerability-influencing factors

Barriers associated with susceptibility or coping capacity can furthermore be associated with different factors influencing the vulnerability. These factors and the barriers associated with them can be classified in one of three categories of *influencing factors*: 1) Technical factors, 2) human-related factors (related to the work force of the system operator), and 3) organizational factors. For instance, whereas the technical condition of a component is a technical factor influencing the susceptibility, the vulnerability is also influenced by the competence that the work force has on condition assessment. Moreover, the inspection and maintenance efforts of the operator is in turn influenced by the income regulation of the operator, which is an organizational vulnerability-influencing factor. In addition, the coping capacity can be negatively influenced by external factors, for instance adverse weather conditions that hamper repair activities or strained operation that renders reserves and corrective actions insufficient. Examples of vulnerability influencing factors are given in Table 2.

3.4. Relationship with power system resilience

The concept of power system vulnerability described above can be related to the concept of power system resilience. Literature shows that resilience is defined and interpreted in different ways, both within risk analysis [42] and resilience engineering [50,51] in general, and within its application to power systems, e.g. [14,22,51–54]. One

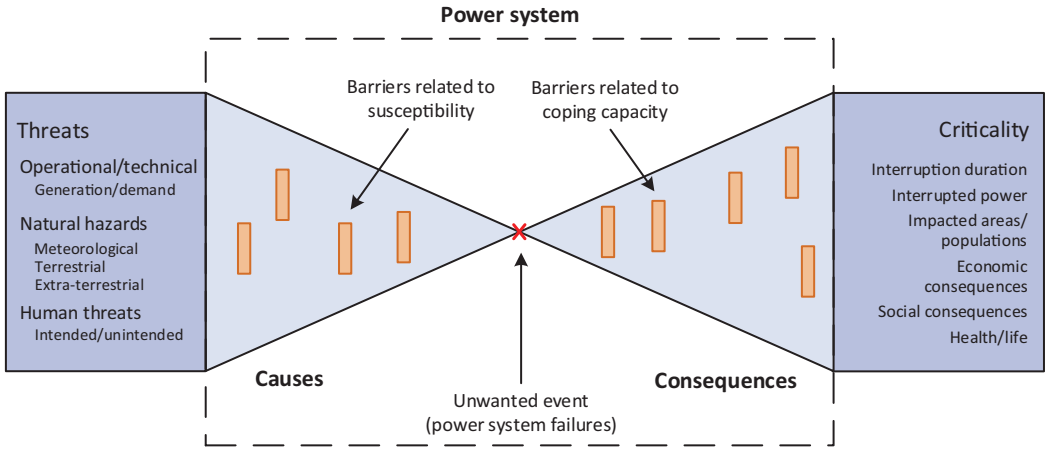

Fig. 3. Bow tie model associated with power system vulnerability.

characterization of resilience commonly used in the literature [50] includes the two dimensions i) *robustness*, "the extent of system function that is maintained", and ii) *rapidity*, "the time required to return to full system operations and productivity" [55]. The relationship with the terms used in the vulnerability analysis framework is illustrated in Fig. 4. On the left-hand side, Fig. 4a shows schematically the time development of a power supply interruption event with the two-dimensional consequences interrupted power and interruption duration as discussed in Section 2. The amount of *interrupted power* is related to the *robustness* of the power system, i.e., it corresponds to the "reverse of" "the extent of the system function that is maintained", whereas the *interruption duration* corresponds to the *rapidity*.

Fig. 4b shows a two-dimensional diagram similar to the consequence diagram in Fig. 1, where extraordinary events are found in the region with high interrupted power and/or long interruption duration. Occurrences of extraordinary events therefore imply that the power system has low values of robustness and/or high values of rapidity (interruption duration) and consequently low resilience. In the context of the vulnerability framework, we therefore find it useful to understand power system resilience as being the inverse of or the dual to power system vulnerability. Hence, the proposed definition of resilience in line with the presented vulnerability analysis framework is that *resilience is an expression for the ability of a system to maintain its function if a threat leads to an unwanted event and the ability of the system to resume its activities after the event occurred*. In other words, high resilience implies low vulnerability and vice versa (as illustrated in Fig. 4b).

3.5. Incorporation of functional models of the physical behaviour of the power system

There is a growing consensus that (a) one needs functional models of the physical behaviour of the critical infrastructure (here: power system) to analyse its vulnerability, and (b) that there is not a single model of the system that is most appropriate for all purposes [1,5]. For this reason, the conceptual framework described above is designed to incorporate different system-specific models and methods for analysing causes and consequences of power system failures. This is illustrated schematically in Fig. 5, where the bow tie model from Fig. 3 has been overlaid with exemplary models for the causes and consequences of a power system failure.[1] Fig. 5 additionally illustrates how the performance of the system (the power supplied to end-users) may vary over time throughout a blackout event (i.e. an extraordinary event) [49]. Another aspect of power systems included in Fig. 5 that is important to capture in models for vulnerability analysis, is the *operating state* of the system at the time of the failure. The operating state is defined as the system state valid for a period of time, characterized by load and generation composition including the electrical topological state (breaker positions etc.) and import/export to neighbouring areas [45].

In the analysis of the consequence of a power system failure one may distinguish between purely structural (or topological) and functional models of the system [15]. A functional model of a power system also represents the physical flow of electric power in the grid[2] and the system's response to failures, and different functional models are classified and compared in [56]. Much of the research related to power system vulnerability has focused on topological models that primarily capture the topological state of the power system [5,17], but it has been established that such models often are not adequate for many of the purposes of vulnerability analysis, cf. e.g. [57,56,58,59,5,1]. To analyse power systems, one also has to model the state of the system in terms of the physical power flow. Quasi-static simulations can capture the transition between operating states with different topologies and/or power flow, and one can incorporate models of the effect of corrective actions (barriers) on the operating state. However, more detailed dynamic simulations considering development of the system state over shorter time scales of the order of milliseconds may be necessary to capture dynamic phenomena related to power system instability (i.e. frequency instability, voltage stability or rotor angle instability) [4,60]. Other functional models addressing complexities related to non-technical aspects of the power system are reviewed and discussed in [1,5,37]. Examples include Agent-Based Modelling, capturing interactions between the human, software and hardware parts of the system and its environment, and Human Reliability Analysis, modelling the performance of human operators and how it depends on the situation and context. The selection and incorporation of appropriate functional models for studies of real power systems is exemplified in Section 6.

4. Vulnerability assessment methodology

Conventional risk assessments typically start by identifying threats and then the sequences of events (scenarios) they may cause [61],

[1] Note that although fault trees and event trees are chosen in Fig. 5 to depict generic causal and consequence models, respectively, such basic models are not by themselves adequate to model the complexity of the power system [1,37]. Relevant methods and models are briefly reviewed and discussed in the following.

[2] The physical power flow in the grid is governed by Kirchhoff 's laws and can be described by a nonlinear set of power flow equations for the voltage at the buses (or nodes) of the grid. These power flow equations and linearized versions of them are examples of functional models of the power system.

Table 1
Classification of barriers reducing power system vulnerability.

Type of action associated with the barrier	When action is taken	Vulnerability dimension affected by barrier	Effect of barrier	Examples of barriers
Preventive action	Prior to power system failures	Susceptibility	Reduce the probability of power system failures	Condition monitoring, preventive maintenance, vegetation management, overload prevention
		Coping capacity	Put the power system in a state better able to cope with power system failures	Preventive generation scheduling, grid reconfiguration (in system operation), grid reinforcement (in system planning)
Corrective action	After power system failures	Coping capacity	Reduce the consequence of power system failures (primarily interrupted power)	Emergency generation rescheduling, emergency HVDC (high-voltage direct current) power, system protection schemes, controlled load shedding.
Restorative action	After power system failures	Coping capacity	Reduce the consequence of power system failures (primarily duration)	Generator black-start capability, grid reconfiguration, availability of spare parts and equipment for repair, competent personnel for system restoration

moving from the left to the right in the bow tie model illustrated in Fig. 3. Finally, a consequence and a probability are then typically assigned to each sequence of events. In contrast to conventional risk assessments, the proposed vulnerability assessment methodology is more concerned with identifying vulnerabilities related to the events with critical consequences and low probabilities. Such events and their consequences are easily missed in conventional risk assessment, partly because (a) the probability of these sequences of events is regarded as negligible, (b) the number of sequences of events to consider otherwise becomes unmanageable, or (c) relevant causal mechanisms are unknown or not considered [13].

To address these shortcomings, we here propose a vulnerability assessment methodology that is complementary to conventional risk assessment and that aims to provide additional insight and decision support particularly related to extraordinary events. Simply put, the underlying idea is to start with identifying possible critical consequences and then move leftwards in the bow tie model, essentially reversing the steps outlined for a conventional risk assessment in the preceding paragraph. The objective is to identify vulnerabilities that should be given attention by the stakeholders (e.g. the system operator) and to identify barriers that may reduce these vulnerabilities. The overall methodology is outlined in [35] and formulated schematically as a sequence of six general steps in the flowchart in Fig. 6.

Because the assessment methodology is centred around “critical” consequences, it is decisive for each application of the methodology to first define the term “critical” and which loads that are regarded as critical loads. As explained in Section 2, what is regarded as “critical” must be determined by, or together with, the relevant stakeholders in the area under study. Contingencies potentially leading to these critical consequences are in the following referred to as *critical contingencies*.

In applications of the methodology, various qualitative and quantitative methods can be employed for the individual steps described generally in Fig. 6. A more extensive survey and discussion of relevant methods can be found in [35], and the application of the methodology is exemplified in Section 6. For instance, step 2 may involve methods for contingency analysis (incorporating functional models as described in Section 3.4) and contingency screening [62], and should also consider common-cause and dependent events [63]. In addition, the step may also involve the identification of the *critical operating states* that, in combination with critical contingencies, may lead to the critical consequences. Step 3 may involve models and assessment of the threat exposure at specific locations, as e.g. in [20,21,23,47]. Step 4 needs to consider what barriers that would have to fail to i) go from exposure of a threat to a critical contingency and ii) from the critical contingency to the critical consequences. Step 5 then needs to consider what could make the barriers identified in step 4 fail. Step 6 results in an overall assessment of the vulnerability, including identified measures for reducing the vulnerability by introducing or strengthening barriers aiming to prevent critical contingencies and/or to reduce the consequences of critical contingencies.

The proposed vulnerability assessment methodology is intended to guide the analyst and the stakeholders, structuring the analysis, and facilitating the identification process. Thus, it allows identifying vulnerabilities related to extraordinary events that, although considered unlikely, are still within the realm of possibility. In addition, such an assessment provides input to stakeholders that is useful to prioritize between which events, vulnerabilities and barriers they should devote most of their attention and resources to. For a more quantitative basis for decision making in such cases, the vulnerability assessment can be supplemented by the estimation of vulnerability indicators, as described in the next section.

5. Vulnerability indicators

This section concerns the development of vulnerability indicators able to measure quantitatively the factors identified to determine the

Table 2
Classification of vulnerability-influencing factors with examples.

Influencing factors	Susceptibility	Coping capacity
Technical	Technical condition of components Operational stress	Equipment for repair Spare parts
Human related (work force)	Availability of skilled personnel Competence with condition assessment	Availability of personnel Operative competence and situational awareness Skills in system restoration and repair of critical components
Organizational	Availability of information Coordination between system operators Structure of the electric energy sector Economic regulation	Availability of communication Coordination of restoration Contingency plans Operational security limits

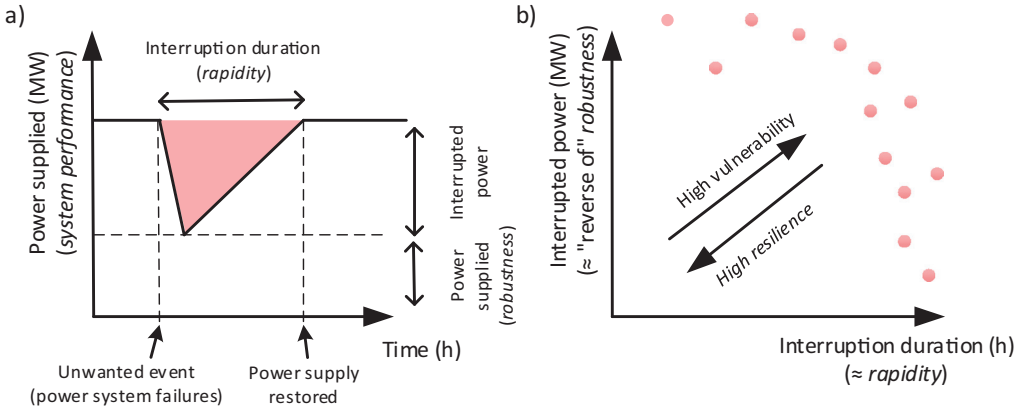

Fig. 4. (a) Schematic time development of a power interruption event (extraordinary event) with general resilience engineering terminology in *italics*; (b) conceptual relationship between power system vulnerability and resilience in terms of the two consequence dimensions introduced in Fig. 1.

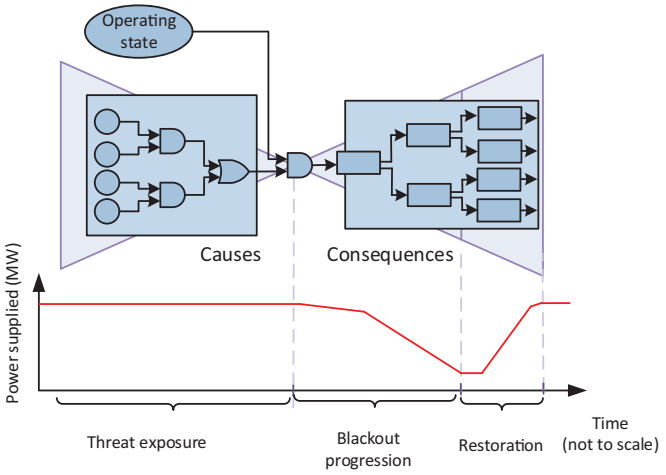

Fig. 5. Illustration of the incorporation of specific (quantitative) methods in the conceptual vulnerability framework.

vulnerability. Vulnerability indicators are also necessary for monitoring how the vulnerability of a power system evolves over time. For an extensive description of the development process, including how indicators can be defined mathematically, calculated based on available data, combined and aggregated, we refer to [29,33,34]. In this article we focus on describing the selection of vulnerability indicators based on the framework for vulnerability analysis described above.

A review of the literature has shown that very few indicators on an aggregate level have been developed to monitor and describe the vulnerabilities in quantitative terms [64]. The kind of indicators that are available and commonly used are reliability indices such as fault frequency, expected energy not supplied, and expected interruption costs. Fig. 7 illustrates how these indicators cover different dimensions of vulnerability according to the conceptual framework described in Section 3. For instance, fault frequency is a measure of both the (external) threat exposure and the (internal) susceptibility of the power system. Thus, one cannot easily disentangle fault frequency data to quantify each of these two dimensions in isolation. And whereas expected interruption costs include useful information about the societal consequences for different end-users, it entangles and encompasses several other underlying factors. Thus, it is by itself not very useful for a detailed analysis of vulnerability. Furthermore, these reliability indices are designed as measures of reliability of supply rather than vulnerability, and in other words, these indicators are better suited for the analysis of ordinary (frequent) events than of extraordinary events.

To address the challenges outlined above, we propose the following principles for the development of vulnerability indicators: 1) The

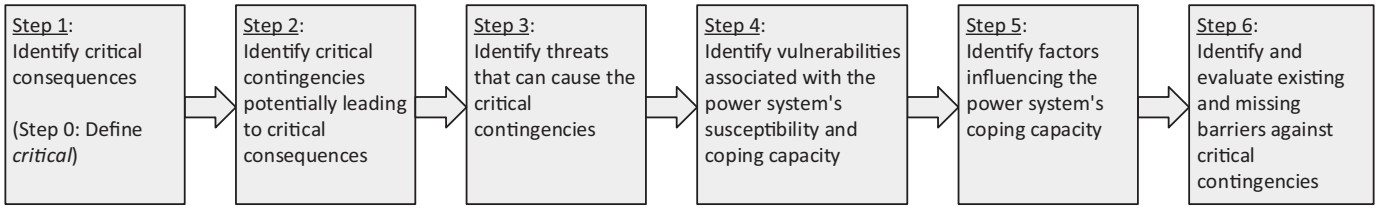

Fig. 6. Flow chart describing schematically the process for the proposed vulnerability assessment methodology.

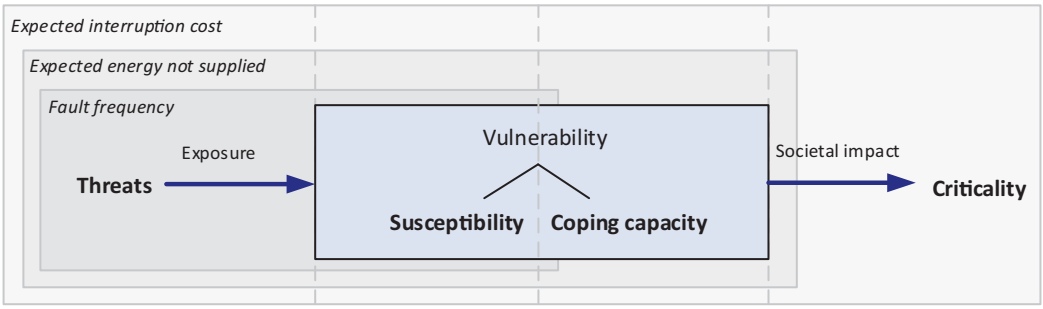

Fig. 7. Examples of indicators covering several dimensions of vulnerability in power systems.

Table 3
Examples of aspects of the vulnerability for which quantitative vulnerability indicators can be developed, associated with different vulnerability dimensions.

Threats	Susceptibility	Coping capacity	Criticality
Wind speed	Localization with respect to threat exposure	Effectiveness of corrective actions	Categories and interruption costs of end-users affected
Precipitation and temperature (risk of icing)	Technical condition of components	System control centre competence	Localization of critical loads
Lightning	Condition assessment competence	Availability of spare parts	Dependence of other critical infrastructures on electricity supply
Degree of line overload	Co-location of cables or other infrastructures in the same trench	Accessibility for repair	Outdoor temperature
Construction activity		Availability of backup generation	
Transportation activity			

development needs to reflect the purpose of the indicators and should hence be carried out in close collaboration with stakeholders; 2) the indicators should be able to give insight into vulnerability related to extraordinary events; 3) they should quantify aspects associated with one of the four dimensions of vulnerability in isolation; and 4) they should be selected based on the aspects identified as relevant for the system of interest. Some examples of aspects of the vulnerability covering each of the vulnerability dimensions are shown in Table 3. For a specific case, the aspects that are relevant can be identified using a vulnerability assessment as described in Section 4, and vulnerability indicators can subsequently be selected and developed for these aspects. This is exemplified more concretely in Section 6.3, where four possible indicators are described for a real case. Note that threat indicators and susceptibility indicators are primarily related to specific threats, whereas indicators for coping capacity and the criticality can cover different threats. The susceptibility and coping capacity indicators can be further categorized as being related to technical factors (e.g. technical condition), human-related factors (e.g. system control centre competence) or organizational factors (e.g. coordination and contingency plans for backup generation), cf. Table 3.

6. Applications to real power systems

This section demonstrates and exemplifies how the vulnerability framework and its components can be applied to real power systems. Table 4 gives an overview of the applications that are described in more detail below. Three of these applications (1–3) are described in separate subsections: Section 6.1 describes a vulnerability assessment relevant for a synchronous area (covering several countries with transmission systems operated with synchronized frequencies), Section 6.2 describes a vulnerability assessment for a transmission system (in one country), and Section 6.3 describes a vulnerability assessment and vulnerability indicators for a regional distribution system (in a region of a country). Each subsection summarizes the vulnerability assessment structured in the six steps described in Section 4. These studies demonstrate that the framework is applicable to power systems at different levels and of different scale, and they illustrate that the methods applied in each case must be adapted to the type of system and the scope of the analysis. Geographical details are anonymised due to confidentiality and the sensitive nature of the studies.

For the two last applications (4 and 5) listed in Table 4, we only include a brief summary in this article and refer to [69–71] for the details:

Reference [69] describes the development of indicators for

Table 4
Overview of applications of the framework for vulnerability analysis to real power systems.

Application	Scope	Components of framework that are applied	References
Vulnerability analysis of HVDC interconnector contingencies	Nordic power system	Vulnerability assessment, incorporating dynamic power system simulations	[65–67]
Risk and vulnerability study of a 420 kV transmission system	National (transmission) power system	Vulnerability assessment, incorporating static and dynamic power flow simulations	[68]
Vulnerability study for 132 kV regional distribution system	Regional (distribution) power system	Vulnerability assessment with development of vulnerability indicators	[35]
Industrial application of vulnerability indicators	Substations in regional (distribution) power system	Calculation of vulnerability indicators	[69]
Norwegian fault and interruption data collection and reporting system	National power system	Conceptual framework (definitions and classifications)	[70,71]

screening and monitoring vulnerabilities related to substations. Calculation of these vulnerability indicators is demonstrated for a set of 132/22 kV substations in a real regional distribution system in Norway. The calculation of the indicators is implemented by the regional distribution system operator as a part of their emergency preparedness work and thus represents an industrial application of the vulnerability indicators described in this article.

Reference [70] describes the standardized fault and interruption data collection and reporting system FASIT that is implemented by all grid companies and the system operator in Norway for the power system at both the transmission and distribution level. Some of the definitions and classifications in the FASIT standard [71] are based on the conceptual framework described in Section 3. Referring to the power system boundaries illustrated in Figs. 2 and 3, the framework allows for distinguishing between *external causes* (associated with threats) and *internal causes* (associated with susceptibilities) of failures. Both internal and external causes are to be reported according to the FASIT standard. To illustrate the distinction by a simple example, consider the case of a lattice tower with a loose bracing that results in a line-to-earth short-circuit of an overhead line during a storm. In this case, the external cause of the failure is the storm, and the internal cause is insufficient maintenance of the tower, making the overhead line more susceptible to the storm threat. Maintenance is a barrier that here turned out to be too weak.

6.1. Vulnerability analysis of HVDC interconnector contingencies

In [65], the vulnerability assessment methodology is used to give a broad overview of the vulnerability of the Nordic power system with respect to contingencies involving High-Voltage Direct Current (HVDC) interconnectors connecting the Nordic synchronous area with neighbouring power systems. The system boundaries were in this case defined to envelope the Nordic synchronous area (Norway, Sweden, Finland and Eastern Denmark), illustrated schematically in Fig. 8. The unwanted event was defined as the outage occurrence of one or more HVDC interconnectors connecting the Nordic synchronous area and another synchronous area. To assess the consequences of such events, it is necessary to consider the following functional aspects of the power systems: i) the frequency will change rapidly in response to the event, depending on the amount of power transmission lost at the outage occurrence and on the operating state of the system; and ii) the reserves and system protection schemes (SPSs) that respond to the changes in frequency to prevent frequency instability and system blackout. A relevant characteristic of the operating state in this case is the inertia of the power system, which simply put depends on the amount of synchronous rotating machines connected to the power system.

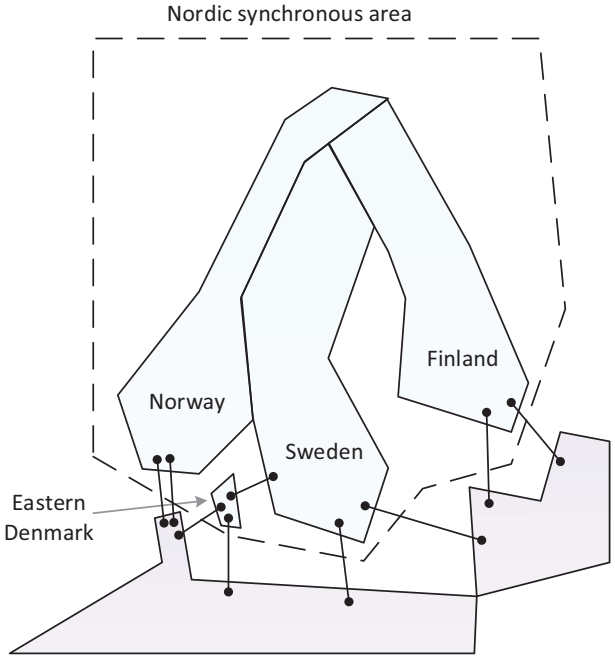

Fig. 8. Schematic of the Nordic synchronous area with interconnections to other synchronous areas. (Only a subset of actual HVDC interconnectors is shown in the figure.).

Step 1: The critical consequences were determined based on the levels of criticality determined in the earlier and more general vulnerability analysis carried out for the Nordic power system [11]. For the rest of the vulnerability assessment, critical consequences were defined as blackouts of (parts of) the Nordic synchronous area following from loss of HVDC power transmission greater than for the so-called reference incident for the system.
Step 2: The method for identifying critical contingencies employed in [65] was a semi-quantitative approach based on enumeration of common-cause contingencies and considerations on the frequency stability of the Nordic synchronous area. Based on the conclusions of [65], more detailed quantitative analysis methods were implemented in [66,67] to assess the consequences of potentially critical HVDC contingencies. These consequence analysis methods include simulation of power system dynamics and capture the inertial response and relevant SPSs. Static power flow simulation was less relevant to consider in the consequence analysis since frequency instability was the main issue given the scope of this study.
Step 3: The system boundaries chosen for this study implies that neighbouring power systems, e.g. the Continental European synchronous area, were defined as external to the power system under study. Thus, the Nordic synchronous area is exposed to operational/technical threats arising from the neighbouring power systems. Blackouts in neighbouring power systems were identified as a threat that could cause the simultaneous outage occurrence of multiple HVDC interconnectors.
Step 4: An important vulnerability is that system inertia may be insufficient to slow the change in system frequency enough for reserves to react to avoid under-frequency load shedding. This is a vulnerability associated with the (lack of) coping capacity of the power system.
Step 5: The amount of system inertia is an important factor influencing the coping capacity. The inertia in turn depends on aspects of the operating state such as total system load, the amount of wind power generation, and the amount of HVDC power import. Since the inertia generally will be lower when the amount of HVDC import is higher, the system generally has lower coping capacity when the potential severity of HVDC contingencies is higher.
Step 6: Inertial response is a barrier associated with the coping capacity that was identified as being weak. Limitation of import or activation of event-driven SPSs based on real-time inertia monitoring (preventively improving coping capacity) is also a potential barrier. Another potential barrier identified in the qualitative vulnerability assessment was fast-acting load-based reserves (also referred to as fast frequency reserves or emergency demand-response, correctively improving coping capacity). Consequently, it was implemented as a SPS barrier in the quantitative consequence analysis [67] (cf. the right-hand side of Fig. 5), and using dynamic power system simulations it was found to be a promising barrier if the time-delay for activation is sufficiently low (up to a few seconds) and the amount of load involved is sufficiently high.

6.2. Risk and vulnerability study of a 420 kV transmission system

In this section, the vulnerability assessment methodology is applied in a case study of a real 420 kV transmission system carried out in close

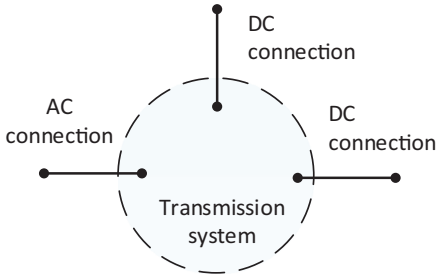

Fig. 9. Transmission system with connections to neighbouring transmission systems.

collaboration with the TSO. The study was first described in [68] within a previous version of the framework. The transmission system is part of a larger synchronous area and is connected to other parts of this synchronous area by a double-circuit AC connection. In addition, the transmission system is connected to other synchronous areas by two HVDC connections. The system is illustrated schematically in Fig. 9.

Step 1: A consequence that would be critical for the TSO is the blackout of the entire transmission system. In such cases, it would typically take several hours to restore the operation of the system.
Step 2: Combinations of critical operating states and critical contingencies (i.e. unwanted events) that could result in system blackout were identified through a combination of generic and power system specific methods: interviews with experts at the TSOs control centre and planning department were carried out to get a broad overview of the system, identified possible sequences of events were structured as an event tree, and the consequences of sequences of events were assessed quantitatively using static and dynamic power flow simulations. Resulting from this, the unwanted event considered for the rest of the analysis was defined as the outage occurrence of both AC lines if import on the AC lines exceeded 900 MW.
Step 3: Threats that could lead to the loss of both AC lines were identified by expert judgement and include: unwanted unselective breaker tripping, substation or bus bar faults (technical/operational threats); transportation accidents, sabotage (unintended and intended human threats, respectively); thunderstorms, galloping lines (natural hazards). Furthermore, these threats were analysed quantitatively by constructing a fault tree model, with input data based on fault statistics combined with expert judgement.
Step 4: One vulnerability is that the two AC lines could be inadvertently connected to the same substation bus bar, which makes the double-circuit AC connection susceptible to bus bar faults leading to common-cause outage of both lines. Another vulnerability associated with coping capacity is the need for manual intervention to carry out certain corrective actions (e.g. activating HVDC emergency power[3]).
Step 5: Examples of factors influencing the power system's coping capacity include situational awareness and operator competence with carrying out corrective actions.
Step 6: Barriers that reduce the consequences of the unwanted event include activating HVDC emergency power, emergency load shedding and controlled islanding of the transmission system. These barriers were furthermore modelled quantitatively by constructing an event tree, in which probabilities of the barriers' success or failure were assigned based on expert judgement.

[3] HVDC emergency power is an automatic or manual corrective action (or system protection scheme) involving relatively rapidly decreasing or increasing the power flow across an HVDC connection.

6.3. Vulnerability study for a 132 kV regional distribution system

In this section, the framework for vulnerability analysis is applied in a case study of a 132 kV distribution power system in a region of Norway, carried out in close collaboration with the regional distribution system operator. Based on an initial evaluation process carried out for the region, an area covering the small towns A, B and C was selected for a closer assessment of potential vulnerabilities. The 132 kV double-circuit overhead power lines A–B and B–C are connecting these regional load centres. The system thus has the simple topology shown in Fig. 10. Parts of the analysis of this case was also presented previously in [35].

Step 1: The system operator regards power interruptions of remote local communities in their region lasting for more than a few days as critical. The critical consequences identified for this case study were therefore long-lasting power interruptions (more than a few days) of critical loads in towns B and C.
Step 2: The critical contingency, leading to critical consequences for town C, is the outage of power line B–C. Since B–C is a double-circuit overhead line, this would require tower breakdown or some other common-cause failure of both circuits involving permanent breakage of both power lines. In case of outage of A–B, supply to B (and C) can be restored by reconfiguration of the underlying distribution grid, but outage of B–C would leave C without backup power supply. Both these contingencies were believed to imply interruption of power supply of up to four days and thus, consequences that were critical according to the operator's definition. For the radial structure of the distribution system in this case, the identification of critical contingencies does not require detailed quantitative analysis, and we can focus on other aspects. However, the case demonstrates the importance of taking common-cause outages into account.
Step 3: Threats that could potentially cause the critical contingencies were identified as snow, icing, thunderstorms and corrosion. Although it is not regarded plausible that each threat in isolation would cause tower breakdown, heavy precipitation and icing combined with strong winds have previously caused similar power line outages in Norway [32]. This particular power line was not found to be likely to be exposed to other natural hazards or to human threats or threats related to operational conditions.
Step 4: Identified vulnerabilities with respect to the contingencies and threats above were poor technical condition (associated with susceptibility) and low accessibility due to the remoteness of the area (associated with coping capacity) along parts of the power line. Two power lines on the same towers is another evident vulnerability.
Step 5: The coping capacity can be influenced by bad weather and lack of daylight, factors which are correlated and likely to coincide during the winter season in Norway. Damage to other infrastructure from natural hazards may also hamper repair and restoration efforts. For instance, heavy snow on forest roads may exacerbate the vulnerability related to accessibility.
Step 6: A potential but missing barrier identified to reduce the susceptibility is improved condition monitoring of towers along the identified segment of the power line B–C. Relevant barriers to improve coping capacity are ensuring available equipment for transportation and repair, a competent crew available, and training and contingency plans for the situation described under step 5. These barriers are associated with power system restoration and address technical, human-related and organizational-related factors influencing the vulnerability, respectively. Other barriers that would improve coping capacity are emergency preparedness measures such as ensuring backup generation for critical loads in town C.

Development of vulnerability indicators: Finally, we illustrate how vulnerability indicators were developed for this study to quantify

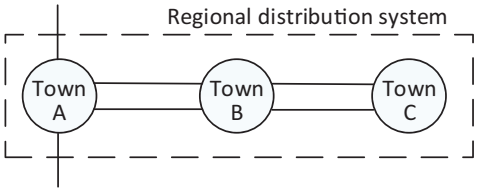

Fig. 10. Grid topology of regional distribution system case.

aspects covering all four dimensions of power system vulnerability. For the sake of brevity, we in this article only outline how these four indicators were selected and quantified, and we refer to [29] for numerical results and further details:

1) *exposure* (related to threats): This indicator quantifies the location-dependent exposure to the threats identified as relevant in the vulnerability assessment described above. Failure data for the power lines and weather data for the area did not give indication of particularly adverse exposure to natural hazards. Values were set lower for some towers due to marine sediments causing corrosion of tower wires.[4] Lower indicator values imply a higher contribution to vulnerability.
2) technical *condition* (related to susceptibility): The technical condition indicator for the tower was set to one of five deterioration states based on inspection data from the asset management system of the operator.
3) *accessibility* for repair (related to coping capacity): The value was set based on local knowledge, with the lowest value meaning "extremely inaccessible" with regards to repairing the towers.
4) *criticality* of consequences of failure: Indicator values for the consequences to society of a tower failure were determined based on the location of critical loads and possibilities for grid reconfiguration. The lowest value was given to towers on power line B–C since breakdown of these towers potentially result in power interruptions for several days for town C.

For this case, the towers for which the combination of indicators 1–4 indicated the lowest contribution to vulnerability were towers on power line B–C [29]. However, the analysis also revealed that those towers on B–C with the worst accessibility were *not* the towers with the worst condition, which means that these factors did not conspire to make the system as vulnerable as one might otherwise fear.

7. Concluding remarks

This article describes a comprehensive framework for analysing the vulnerability of power systems with respect to extraordinary events. As the vulnerability of power systems is a highly complex and multi-dimensional topic, it requires a broad description that encompasses all relevant aspects. Three main components of the vulnerability analysis framework have been presented: (1) A conceptual framework that classifies aspects of the vulnerability of a power system according to four dimensions, namely the internal dimensions of the power system's (i) susceptibility and (ii) coping capacity, and the external dimensions related to (iii) threats and (iv) the criticality of societal consequences. (2) A general methodology for vulnerability assessment that starts by identifying possible critical consequences. (3) Vulnerability indicators for quantifying and monitoring the vulnerability of power systems that cover all four dimensions described under (1).

A summary of applications of the framework has demonstrated how these three components can be applied together on real power systems to provide a structured basis for prioritization and decision making. Specifically, the implementation of the analysis framework guides the analysts and stakeholders in uncovering dependencies and influencing factors and in identifying barriers to be introduced or strengthened to reduce the vulnerability of the power system. The conceptual framework and the associated nomenclature furthermore serve as a basis for understanding and communicating about vulnerabilities and extraordinary events.

Through continuously testing and applying the vulnerability analysis framework, we have established the importance of adapting the analysis to the power system under study. Although the framework is general and provides a unified structure to the vulnerability analyses, an appropriate combination of qualitative and quantitative techniques must be employed to capture the physics and characteristic aspects of the particular power system. One key insight is that it is valuable to complement detailed, quantitative analysis with more qualitative initial assessments, as enabled by the proposed vulnerability analysis framework.

[4] Tower wires or guy-wires are tensioned cables anchoring the tower to the ground to support and stabilize it.

Declaration of Competing Interest

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

Acknowledgements

This work was supported in part by the Research Council of Norway under Grant 191124 ("the Vulnerability project") and Grant 255226 ("the HILP project") and in part by Statnett (the Norwegian Transmission System Operator), Fingrid (the Finnish Transmission System Operator), Norwegian Water Resources and Energy Directorate, Norwegian Directorate for Civil Protection, Energy Norway and grid companies. The authors would like to thank project partners and collaborators for discussions, comments and contributions to the work leading up to this article.

References

[1] Zio E. Challenges in the vulnerability and risk analysis of critical infrastructures. Reliab Eng Syst Saf 2016;152:137–50. https://doi.org/10.1016/j.ress.2016.02.009.
[2] Commission of the European Communities. Green paper on a European programme for critical infrastructure protection. 2005. Brussels.
[3] Kröger W, Zio E. Vulnerable systems. London: Springer; 2011.
[4] Pourbeik P, Kundur PS, Taylor CW. The anatomy of a power grid blackout - Root causes and dynamics of recent major blackouts. IEEE Power Energy Mag 2006;4:22–9. https://doi.org/10.1109/MPAE.2006.1687814.
[5] Abedi A, Gaudard L, Romerio F. Review of major approaches to analyze vulnerability in power system. Reliab Eng Syst Saf 2019;183:153–72. https://doi.org/10.1016/j.ress.2018.11.019.
[6] Kjølle GH, Samdal K, Singh B, Kvitastein OA. Customer costs related to interruptions and voltage problems: methodology and results. IEEE Trans Power Syst 2008;23:1030–8. https://doi.org/10.1109/TPWRS.2008.922227.
[7] Svegrup L, Johansson J, Hassel H. Integration of critical infrastructure and societal consequence models: impact on swedish power system mitigation decisions. Risk Anal **9**, 2019. https://doi.org/10.1111/risa.13272. 1970-1996.
[8] Kjølle GH, Utne IB, Gjerde O. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. Reliab Eng Syst Saf 2012;105:80–9. https://doi.org/10.1016/j.ress.2012.02.006.
[9] Bompard E, Huang T, Wu Y, Cremenescu M. Classification and trend analysis of threats origins to the security of power systems. Int J Electr Power Energy Syst 2013;50:50–64. https://doi.org/10.1016/j.ijepes.2013.02.008.
[10] Dobson I, Carreras BA, Lynch VE, Newman DE. Complex systems analysis of series of blackouts: cascading failure, critical points, and self-organization. Chaos 2007;17:026103https://doi.org/10.1063/1.2737822.
[11] Doorman GL, Uhlen K, Kjølle GH, Huse ES. Vulnerability analysis of the Nordic power system. IEEE Trans Power Syst 2006;21:402–10. https://doi.org/10.1109/TPWRS.2005.857849.
[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;39:6308–20. https://doi.org/10.1016/j.enpol.2011.07.030.
[13] Aven T. Ignoring scenarios in risk assessments: Understanding the issue and improving current practice. Reliab Eng Syst Saf 2016;145:215–20. https://doi.org/10.1016/j.ress.2015.08.012.
[14] Panteli M, Mancarella P. The grid: stronger, bigger, smarter?: presenting a

conceptual framework of power system resilience. IEEE Power Energy Mag 2015;13:58–66. https://doi.org/10.1109/MPE.2015.2397334.
[15] Johansson J, Hassel H, Zio E. Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems. Reliab Eng Syst Saf 2013;120:27–38. https://doi.org/10.1016/j.ress.2013.02.027.
[16] Bompard E, Pons E, Wu D. Analysis of the structural vulnerability of the interconnected power grid of continental Europe with the Integrated Power System and Unified Power System based on extended topological approach. Int Trans Electr Energy Syst 2013;23:620–37. https://doi.org/10.1002/etep.1618.
[17] Cuadra L, Salcedo-Sanz S, Del Ser J, Jiménez-Fernández S, Geem ZW. A critical review of robustness in power grids using complex networks concepts. Energies 2015;8:9211–65. https://doi.org/10.3390/en8099211.
[18] Landegren F. Technical infrastructure networks as socio-technical systems: addressing infrastructure resilience and societal outage consequences. PhD thesis Lund University; 2018.
[19] Veeramany A, Unwin SD, Coles GA, Dagle JE, Millard DW, Yao J, et al. Framework for modeling high-impact, low-frequency power grid events to support risk-informed decisions. Int J Disaster Risk Reduct 2016;18:125–37. https://doi.org/10.1016/j.ijdrr.2016.06.008.
[20] Veeramany A, Coles GA, Unwin SD, Nguyen TB, Dagle JE. Trial implementation of a multihazard risk assessment framework for high-impact low-frequency power grid events. IEEE Syst J 2017:1–9. https://doi.org/10.1109/JSYST.2017.2737993.
[21] Ciapessoni E, Cirio D, Kjølle G, Massucco S, Pitto A, Sforna M. Probabilistic risk-based security assessment of power systems considering incumbent threats and uncertainties. IEEE Trans Smart Grid 2016;7:2890–903. https://doi.org/10.1109/TSG.2016.2519239.
[22] Watson J-P, Guttromson R, Silva-Monroy C, Jeffers R, Jones K, Ellison J, et al. Conceptual framework for developing resilience metrics for the electricity, oil, and gas sectors in the United States. Albuquerque, New Mexico and Livermore: California: Sandia National Laboratories; 2014.
[23] Panteli M, Pickering C, Wilkinson S, Dawson R, Mancarella P. Power system resilience to extreme weather: fragility modeling, probabilistic impact assessment, and adaptation measures. IEEE Trans Power Syst 2017;32:3747–57. https://doi.org/10.1109/TPWRS.2016.2641463.
[24] Wang Y, Chen C, Wang J, Baldick R. Research on Resilience of power systems under natural disasters—a review. IEEE Trans Power Syst 2016;31:1604–13. https://doi.org/10.1109/TPWRS.2015.2429656.
[25] Jufri FH, Widiputra V, Jung J. State-of-the-art review on power grid resilience to extreme weather events: definitions, frameworks, quantitative assessment methodologies, and enhancement strategies. Appl Energy 2019;239:1049–65. https://doi.org/10.1016/j.apenergy.2019.02.017.
[26] Bialek J, Ciapessoni E, Cirio D, Cotilla-Sanchez E, Dent C, Dobson I, et al. Benchmarking and validation of cascading failure analysis tools. IEEE Trans Power Syst 2016;31:4887–900. https://doi.org/10.1109/TPWRS.2016.2518660.
[27] Vaiman M, Bell K, Chen Y, Chowdhury B, Dobson I, Hines, et al. Risk assessment of cascading outages: methodologies and challenges. IEEE Trans Power Syst 2012;27:631–41. https://doi.org/10.1109/TPWRS.2011.2177868.
[28] Kjølle GH, Gjerde O, Hofmann M. Vulnerability and security in a changing power system – Executive summary. Trondheim: SINTEF Energy Research; 2013. Report no. TR A7278.
[29] Hofmann M, Kjølle GH, Gjerde O. Vulnerability indicators for electric power grids. SINTEF Energy Research; 2013. Report no. TR A7276.
[30] Kjølle G, Gjerde O, Nybø A. A framework for handling high impact low probability events (HILP) events. Proc. 20th Int. Conf. Electr. Distrib. CIRED. 2010.
[31] Johansson E, Uhlen K, Nybø A, Kjølle G, Gjerde OExtraordinary events. understanding sequence, causes, and remedies. Proc. Eur. Saf. Reliab. Conf. (ESREL) 2010. 2010.
[32] Kjølle GH, Gjerde O, Hofmann M. Monitoring vulnerability in power systems – extraordinary events, analysis framework and development of indicators. Proc. 12th Int. Conf. Probabilistic Methods Appl. Power Syst. (PMAPS). 2012. p. 935–40.
[33] Hofmann M, Kjølle GH, Gjerde O. Development of indicators to monitor vulnerabilities in power systems. 11th Int. Probabilistic Saf. Assess. Manag. Conf. Annu. Eur. Saf. Reliab. Conf. 2012 (PSAM11 ESREL 2012). 7. 2012. p. 5869–78.
[34] Hofmann M, Gjerde O, Kjølle GH, Gramme E, Hernes JG, Foosnæs JA. Developing indicators for monitoring vulnerability. Proc. 22nd Int. Conf. Electr. Distrib. (CIRED). 2013.
[35] Kjølle GH, Gjerde O. Vulnerability analysis related to extraordinary events in power systems. 2015 IEEE PowerTech 2015. https://doi.org/10.1109/PTC.2015.7232388.
[36] GARPUR Consortium. D1.1: State of the art on reliability assessment in power systems. 2014.
[37] Kröger W. Securing the operation of socially critical systems from an engineering perspective: new challenges, enhanced tools and novel concepts. Eur J Secur Res 2017;2:39–55. https://doi.org/10.1007/s41125-017-0013-9.
[38] Eurelectric. Power outages in 2003 – task force power outages. Union of the Electricity Industry - Eurelectric aisbl; 2004.
[39] Swedish Energy Agency. Storm Gudrun - What can be learnt from the natural disaster of 2005? 2007.
[40] Hillberg E. Perception, Prediction and Prevention of Extraordinary Events in the Power System PhD thesis Norwegian University of Science and Technology; 2016
[41] Veloza OP, Santamaria F. Analysis of major blackouts from 2003 to 2015: classification of incidents and review of main causes. Electr J 2016;29:42–9. https://doi.org/10.1016/j.tej.2016.08.006.
[42] Society for Risk Analysis. SRA glossary. Society for Risk Analysis, 2015.
[43] Birkmann J. Measuring vulnerability to promote disaster-resilient societies: conceptual frameworks and definitions. In *Measuring vulnerability to natural hazards: Towards disaster resilient societies*. Hong Kong: United Nations University Press; 2006.
[44] UCTE. UCTE Operation Handbook. Union for the Coordination of the Transmission of Electricity (UCTE); 2004.
[45] Kjølle GH, Gjerde O. The OPAL methodology for reliability analysis of power systems. Trondheim: SINTEF Energy Research; 2012. Report no. TR A7175.
[46] Dobson I, Newman DE. Cascading blackout overall structure and some implications for sampling and mitigation. Int J Electr Power Energy Syst 2017;86:29–32. https://doi.org/10.1016/j.ijepes.2016.09.006.
[47] Solheim ØR, Kjølle G, Trötscher T. Wind dependent failure rates for overhead transmission lines using reanalysis data and a Bayesian updating scheme. Proc. 2016 Int. conf. probabilistic methods appl. power syst. (PMAPS) 2016. https://doi.org/10.1109/PMAPS.2016.7764104.
[48] Hollnagel E. Barriers and accident prevention. Ashgate Publishing Company; 2004.
[49] Sperstad IB, Kiel ES. Development of a qualitative framework for analysing high-impact low-probability events in power systems. Eur. Saf. Reliab. Conf. (ESREL) 2018. 2018.
[50] Hosseini S, Barker K, Ramirez-Marquez JE. A review of definitions and measures of system resilience. Reliab Eng Syst Saf 2016;145:47–61. https://doi.org/10.1016/j.ress.2015.08.006.
[51] Righi AW, Saurin TA, Wachs P. A systematic literature review of resilience engineering: research areas and a research agenda proposal. Reliab Eng Syst Saf 2015;141:142–52. https://doi.org/10.1016/j.ress.2015.03.007.
[52] Panteli M, Mancarella P, Trakas DN, Kyriakides E, Hatziargyriou ND. Metrics and quantification of operational and infrastructure resilience in power systems. IEEE Trans Power Syst 2017;32:4732–42. https://doi.org/10.1109/TPWRS.2017.2664141.
[53] Ciapessoni E, Cirio D, Pitto A, Panteli M, Harte M van. Defining power system resilience. CIGRE WG C4.47; 2019.
[54] IEEE PES Industry Technical Support Task Force. The definition and quantification of resilience. IEEE; 2018.
[55] McDaniels T, Chang S, Cole D, Mikawoz J, Longstaff H. Fostering resilience to extreme events within infrastructure systems: characterizing decision contexts for mitigation and adaptation. Glob Environ Change 2008;18:310–8. https://doi.org/10.1016/j.gloenvcha.2008.03.001.
[56] LaRocca S, Johansson J, Hassel H, Guikema S. Topological performance measures as surrogates for physical flow models for risk and vulnerability analysis for electric power systems. Risk Anal 2015;35:608–23. https://doi.org/10.1111/risa.12281.
[57] Hines P, Cotilla-Sanchez E, Blumsack S. Do topological models provide good information about electricity infrastructure vulnerability? Chaos Interdiscip J Nonlinear Sci 2010;20:033122,https://doi.org/10.1063/1.3489887.
[58] Cuffe P. A comparison of malicious interdiction strategies against electrical networks. IEEE J Emerg Sel Top Circuits Syst 2017;7:205–17. https://doi.org/10.1109/JETCAS.2017.2704879.
[59] Eusgeld I, Kröger W, Sansavini G, Schläpfer M, Zio E. The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. Reliab Eng Syst Saf 2009;94:954–63. https://doi.org/10.1016/j.ress.2008.10.011.
[60] Kundur P, Paserba J, Ajjarapu V, Andersson G, Bose A, Canizares C, et al. Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions. IEEE Trans Power Syst 2004;19:1387–401. https://doi.org/10.1109/tpwrs.2004.825981.
[61] Rausand M. Risk assessment: theory, methods, and applications. John Wiley & Sons; 2013.
[62] Ciapessoni E, Cirio D, Pitto A, Kjølle G, Jakobsen SH, Sforna M. Contingency screening starting from probabilistic models of hazards and component vulnerabilities. 2016 Power Syst. Comput. Conf. (PSCC) 2016. p. 1–8. https://doi.org/10.1109/PSCC.2016.7540897.
[63] Papic M, Agarwal S, Allan RN, Billinton R, Dent CJ, Ekisheva S, et al. Research on Common-Mode and Dependent (CMD) Outage Events in Power Systems: A Review. IEEE Trans Power Syst 2017;32:1528–36. https://doi.org/10.1109/TPWRS.2016.2588881.
[64] Hofmann M, Gjerde O, Kjølle GH. Vulnerability in electric power grids: state of the art and framework for vulnerability indicators. SINTEF Energy Research; 2011. Report no. TR A7120.
[65] Sperstad IB, Kjølle GH, Gjerde O, Vrana TK, Jakobsen SH, Turunen J, et al. Vulnerability analysis of HVDC contingencies in the Nordic power system. Proc. 2018 CIGRE Sess. 2018.
[66] Solvang EH. Dynamic simulations of simultaneous HVDC contingencies in the nordic power system considering system integrity protection schemes Master thesis Norwegian University of Science and Technology; 2018
[67] Solvang EH, Sperstad IB, Jakobsen SH, Uhlen K. Dynamic simulation of simultaneous HVDC contingencies relevant for vulnerability assessment of the Nordic power system. 2019 IEEE PowerTech 2019. https://doi.org/10.1109/PTC.2019.8810863.
[68] Gjerde O, Kjølle GH, Detlefsen NK, Brønmo G. Risk and vulnerability analysis of power systems including extraordinary events. 2011 IEEE PowerTech 2011. https://doi.org/10.1109/PTC.2011.6019251.
[69] Gramme E, Eldrup M, Veierud T, Eriksen T. Using indicators to screen and monitor substation vulnerability affecting security of supply. Proc. 2016 CIGRE Sess. 2016.
[70] Kjølle G, Eggen AO, Vefsnmo HM, Heggset J, Bostad A, Trøtscher T, et al. Norwegian disturbance management system and database. Proc. 2016 CIGRE Sess. 2016.
[71] Referansegruppe feil og avbrudd. Definitions related to failures and interruptions in the electric power system (Norwegian: Definisjoner knyttet til feil og avbrudd i det elektriske kraftsystemet). Norwegian Water Resources and Energy Directorate, Energy Norway, Statnett. Oslo: SINTEF Energy Research; 2019.