Electrical Power and Energy Systems 125 (2021) 106408

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

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

A graph-based modelling framework for vulnerability analysis of critical sequences of events in power systems

Iver Bakken Sperstad*, Espen Hafstad Solvang, Sigurd Hofsmo Jakobsen

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

A B S T R A C T

Major blackouts may have critical societal consequences and are very challenging to analyse and mitigate. Part of the challenge lies in the complex sequences of events that characterize such blackouts and that involve a diverse set of mechanisms propagating the events. The analysis is also challenged by the great uncertainties associated with individual mechanisms and thus with the overall likelihood of sequences of event. This article proposes a general framework which uses a graph to describe the causal relationship between consequences, system states, initiating events and barriers. A concrete implementation of the framework is presented by implementing exemplary models for three transition mechanisms, namely i) protection system failures, ii) failure of corrective actions, and iii) failure of islanding. In the implementation, a graph is automatically generated where edges are associated with these transition mechanisms. A vulnerability analysis methodology based on the modelling framework is proposed that allows for identifying how critical consequences might occur as well as estimating their likelihoods of occurring. The vulnerability analysis methodology moreover incorporates a possibilistic uncertainty analysis to explicitly capture uncertainties associated with the likelihood of events. Finally, a case study considering a small but realistic test system is used to illustrate the approach and demonstrate its main advantages: i) The vulnerability analysis can identify critical sequences of events and barriers to mitigate them, ii) the graph-based representation allows for exploring the sequences of events and understanding the vulnerabilities, iii) the modelling framework is general and can incorporate multiple transition mechanisms, and iv) the analysis accounts for the large uncertainty associated with the critical sequences of events.

1. Introduction

Major blackouts occur relatively infrequently but may have critical societal consequences when they do [1–4]. These blackout events can be broadly classified by whether they primarily are due to natural hazards (e.g. extreme weather) or whether they are attributed to more diverse and complex causes [2,3]. The first group is characterized by multiple near-simultaneous weather-related failure events and extensive physical damage to the infrastructure and consequently long restoration times and interruption durations [3]. The second group is characterized by often having a single initiating failure event, followed by complex sequences of causally related events, eventually leading to wide-area power interruptions and large societal consequences [1,5,6]. These sequences of events are sometimes referred to as cascading events, cascading outages or cascading blackouts. Such blackout events can involve a multitude of mechanisms that make the blackout event propagate by transitioning from one system state to another. Examples include such diverse mechanisms as protection and control system failures, failure of corrective actions (including system protection schemes), tripping of overloaded transmission lines, generators losing synchronism and tripping, etc. [6–8].

This article focuses on this second group of major blackouts and emphasizes the view of such a blackout as a sequence of causally related events. To describe such sequences of events, we propose a modelling framework based on concepts from graph theory, and we use this framework to analyse power system vulnerability. *Vulnerability* is a term that has been defined and understood in a variety of ways in the context of power systems [2]. In this article, we broadly understand vulnerability as an expression for the problems the system faces to maintain its function if a threat leads to power system failures [4,9,10], potentially leading to interruption of electricity supply and associated societal consequences. A power system failure can here be the *initiating event* of a sequence of events in the power system. A *barrier* is understood as something that either can prevent a sequence of events from taking place or protect against its consequences, and a vulnerability can be associated with a barrier that is either missing, weak or malfunctioning [4,9,10].

In analysing vulnerability we are most concerned with sequences of events leading to societal consequences that in some sense are *critical*. What consequences are regarded as critical depends on the system and in general has to be determined by or together with the relevant stakeholders, e.g. the system operator, regulators or other authorities [11]. The main objectives of a vulnerability analysis within the proposed framework is to identify *critical sequences of events*, and thus to identify vulnerabilities and in turn effective barriers against such events.

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

https://doi.org/10.1016/j.ijepes.2020.106408
Received 12 November 2019; Received in revised form 1 July 2020; Accepted 27 July 2020

1.1. Related work

Modelling of major blackouts is a complex task, and it is infeasible for one single method to encompass all aspects [2,12]. We will focus on blackouts due to so-called cascading outages, on which extensive research has been conducted. The interested reader may refer to [6,8] for reviews of existing methods. Recent developments on the benchmarking and validation of simulation tools for cascading outages are described in [7,13]. Inspired by classifications e.g. in [2,6,8], we can broadly divide the diverse set of existing methods by the level of detail used for modelling the electrical grid: i) statistical approaches, where the grid is not explicitly represented, ii) topological approaches, where the grid is represented as a graph, and iii) electrical engineering approaches, where the grid is represented and simulated as an electric circuit.

Statistical approaches use statistical methods to predict the blackout size or the number of components in an outage state at each stage of the propagation of the blackout event. Typical examples of the former approach are [14,15], and the latter approach is demonstrated in [16,17], which uses a branching process for estimating the number of outaged components in each stage of the cascade. More recently, [18] uses historical data to help evaluate the credibility of statistical approaches. A recent review of the use of influence or interaction graphs in such approaches is found in [19].

Topological approaches are the type of approaches where graph theory is most commonly used in the analysis of blackouts. However, unlike our work these models represent the power system as a graph, whereas we represent possible sequences of events in a blackout as a graph. An overview of the literature on topological models for vulnerability analysis can be found in [20]. Another review on topological models more generally is provided by [21]. The review in [2] of methods for power system vulnerability analysis in general also includes discussion of methods based on graph theory.

Our work falls within the electrical engineering approach to modelling blackout events. These approaches typically also include some type of stochastic modelling of outage occurrences. However, unlike the purely statistical approaches, electrical engineering approaches simulate how electrical quantities in the power system change as the blackout event propagates. In our work this is combined with a graph-based approach to analysing sequences of events leading to critical consequences. A directed graph is constructed that describes a set of discrete-time Markov chains: Each vertex of the graph represents a contingency state and the edges of the graph are labelled with state transition probabilities.

The graph-based approach proposed in this article has some similarities with the electrical engineering approach in [22], which proposes a Markov model for state transitions in the propagation of a blackout event. The states of the Markov chain represent the contingency state of the transmission lines in the system, but the Markov chains are not explicitly recast to a graph formulation as in our case. An advantage of our approach is that the graph that is generated is stored and utilized in a vulnerability analysis methodology. It is emphasized by [22] that their model allows for finding "critical paths" of the blackout, however without further elaborating on how. In our approach, on the other hand, critical paths are explicitly defined and identified in the vulnerability analysis. Another article using Markov models is [23], where each state represents the number of failed lines and the total capacity of the outaged lines. The approach is extended upon in [24], where an additional parameter representing whether or not the state is stable is introduced. However, unlike our approach, the information on the transition between the states is not stored. A framework based on modelling system trajectories (sequences of events) is proposed in [25], but is applied in a security assessment context rather than a vulnerability analysis context. In [26] graph theory is used in a reliability analysis context to find propagation paths for outages of transmission lines due to protection system failures.

Several methods aim to identify the transmission lines occurring in most critical initiating events and the lines occurring in most subsequent cascading outages [19]. For instance, in [27] a Monte Carlo-like approach is used to show that these two sets of transmission lines do not overlap. This insight inspired works such as [28,29], whose aim was to speed up the Monte Carlo sampling of sequences of events. They did so using Markovian tree search to avoid sampling duplicated states and searching for the states with a major contribution to risk. In [30] a Markovian influence graph is used to count the number of outages at each stage in the same way as [16,17]. In addition to this, [30] suggests a method for calculating the importance of each component in the cascade. In [31], the approach for building influence graphs are generalized by including multiple line outages in the states of the Markov chain.

Other lines of research have used a graph-theoretical approach to the power network inhibition or interdiction problem, i.e. the problem of finding a small set of transmission lines whose outage occurrence could cause major blackouts. For instance, [32] used graph partitioning methods to find subgraphs of the grid with large imbalances, and [33] used graph theory to consider the feasibility boundary of the power flow equations for the system. The latter work was later extended in [34], and more details on this and related work can be found in [35]. However, most work along this line of research analyse multiple contingencies without considering the sequences of events that give rise to them. A more recent review of the power network interdiction problem and intentional attacks can be found in [36].

Previous works as those mentioned above has considered models for various relevant transition mechanisms and barrier failures, such as protection system failure [25,26,37–42] and corrective action failure [25,43–47]. The possible failure to operate in island mode after system separation has also been considered [43,45,48], although most work on that topic seem to consider the optimization of controlled or intentional islanding (see e.g. [49]). Furthermore, most previous work has neglected interactions between different mechanisms and has been limited to consider mechanisms in isolation.

Another challenge that has been addressed only to a limited extent in previous research is accounting for the uncertainties that are inherent in the sequences of events of major blackouts [12]. Several of the works mentioned above include probabilistic models for the transition from one state to another [16,17,22–24]. These capture uncertainty in the sense of variability in the processes governing the transitions (i.e., *aleatory* uncertainties [50]). Some works also account for the variability e.g. in the load of the system under study. Recent work has also started accounting for uncertainty due to lack of knowledge (*epistemic uncertainty* [50]) in vulnerability analysis [51]. However, transition probabilities are associated with deep uncertainties that are typically not reflected in the results from such analyses.

A broader and more general methodology, that is not limited to individual mechanisms, has previously been proposed in [4,9,10]. The underlying idea is to start with identifying possible critical consequences in the power system under study. Using this as a starting point, the next step is to move "backwards" in possible sequences of events to identify critical contingencies and operating states that could lead to such consequences and finally to identify barriers that could mitigate them. An advantage of this approach that we utilize in our work is that it helps one to understand by which sequences of events critical consequences could occur and how they could be mitigated. The methodology incorporates different qualitative and quantitative methods at the various steps of the analysis. Although such an approach can capture a broad set of transition mechanisms on a qualitative level, no quantitative modelling framework has yet been developed on the basis of this methodology.

1.2. Contributions and outline

This article seeks to put the general methodology proposed in

[4,9,10] in a more mathematical framework that allows for quantitative vulnerability analysis. More specifically, the main contributions of the article with respect to related work reviewed in the preceding section can be stated as follows:

1. It proposes a general framework for modelling possible sequences of events leading to power supply interruptions. It is based on constructing a graph that describes the causal relationship between different system states and consequences. Information about transition mechanisms, multiple operating states and prior outages is also encoded in the graph. This sets it apart from previous graph-based contributions reviewed above where only the properties of the power grid is encoded in a graph. Compared to other methods based on Markov models, the graph that is constructed subsequently used to visualize sequences of events and analyse vulnerabilities.
2. Based on this graph-based modelling framework, a vulnerability analysis methodology is proposed. The main novelty of the methodology lies in how it utilizes the graph that is constructed to identify critical sequences of events (associated with paths in the graph) and describe how critical consequences might occur. The methodology furthermore allows identifying vulnerabilities associated with barrier failures (transitions), which distinguishes it from previous work based on Markov models or influence or interaction graphs reviewed above.
3. The framework furthermore allows estimating the expected frequency of occurrence (i.e. the likelihood) of the critical sequences of events *and* the associated uncertainty. These estimates account for time-dependent failure rates of initiating events and conditional probabilities for event propagation, which are encoded in a single graph. The uncertainty analysis thus only requires the graph to be constructed once.
4. The modelling framework is formulated in a general manner that allows implementing several mechanisms for propagating the sequence of events and assessing their interactions and contributions to the vulnerability of the system. A concrete implementation of the framework and its application to vulnerability analysis is demonstrated by implementing exemplary models for three types of mechanisms, namely i) protection and control system failures, ii) failure of corrective actions (generation rescheduling and controlled load shedding), and iii) failure of islanding. This is to our knowledge the first publication where these three barrier failures are taken into account in the same vulnerability analysis.

The rest of the article is structured as follows. Section 2 describes the general graph-based modelling framework and vulnerability analysis methodology. A concrete exemplary implementation of the framework is presented in Section 3. The application of the proposed approach is subsequently illustrated through a case study considering a small but realistic test system in Section 4. The article is concluded in Section 5 with a summary of the advantages that are demonstrated and some suggestions for how the framework could be extended and applied.

2. General modelling framework and vulnerability analysis methodology

The basic idea of the modelling framework is to use concepts from graph theory to model sequences of events in power systems. A graph is constructed to describe how initiating events lead to sequences of transitions between different system states (vertices in the graph) propagated through different transition mechanisms (edges between vertices). These sequences of events can result in different consequences for the power system (also described by vertices in the graph). The overall approach for applying this framework in a vulnerability analysis can be described schematically as shown in Fig. 1.

The following subsections lay the theoretical foundation for the general graph-based modelling framework. Concrete examples of how the graph is constructed according to this framework are given in Section 3.

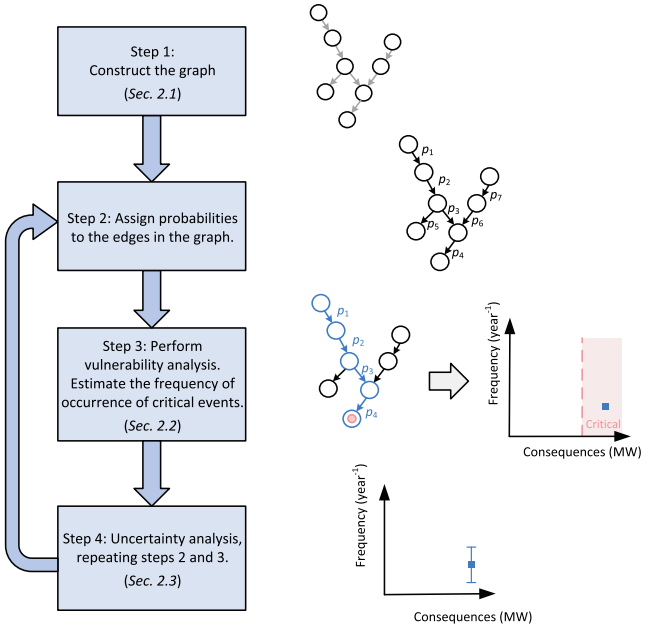

Fig. 1. Schematic illustration of the proposed approach combining a graph-based modelling framework and a vulnerability analysis methodology.

2.1. Graph-based framework for sequences of events

The proposed modelling framework is based on representing sequences of events as paths in a directed acyclic graph [52]. A graph G is in general defined as the ordered pair $G = (V, E)$ of sets of vertices V and edges E. A vertex $v \in V$ in this framework is in a general sense used to represent a state in the power system (to be elaborated below). An edge $e = (v, v') \in E \subseteq V \times V$ in the directed graph describes the transition from the state associated with vertex v to the state associated with vertex v'. A simple example of a graph according to our framework is illustrated in Fig. 2.

A sequence of events is then associated with a path P in the graph G. A path is a subgraph that can be described by a sequence of non-repeating adjacent vertices, $P = (v_0, v_1, \ldots, v_k)$, or equivalently by the sequence of edges joining these vertices. We will denote the set of all possible paths in the graph G by S_P. We will furthermore introduce mappings α: $S_P \rightarrow V$ and ω: $S_P \rightarrow V$ that identify the source vertex $\alpha(P) = v_0$ and target vertex $\omega(P) = v_k$ of a path in a directed graph.

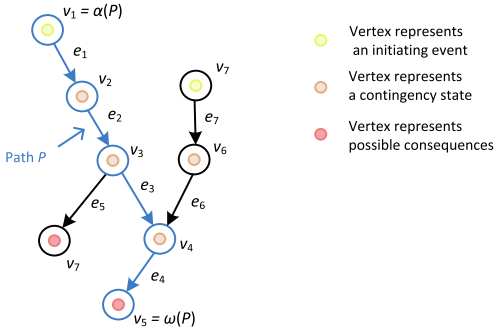

Fig. 2. Example of a graph G and a path $P \in G$ (highlighted in blue) associated with a sequence of events from an initiating event, through contingency states, and leading to consequences. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

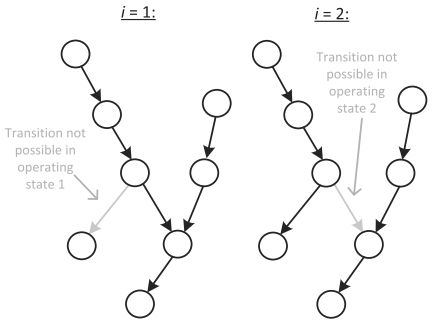

Fig. 3. Example of a graph G describing two operating states and possible sequences of events in each of the operating states.

2.1.1. Multiple operating states

In the framework, information about the operating state of the power system will be incorporated in the graph. The same graph G is thus used to describe all operating states under consideration. A path may describe a sequence of events that is possible when the system initially is in one operating state but not possible in another. We let the index $i \in I$ identify the initial operating state of the system. This is illustrated in Fig. 3, where P describes a sequence of events that is possible for $i = 1$ but not possible for $i = 2$. A sequence of events is thus not unambiguously identified by the path P alone, but is described in the framework by the pair $(P, i) \in S_P \times I$.

An operating state is generally defined as "a 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" [40]. For our purposes we will define and distinguish between two components of this operating state: 1) The *contingency state* C describes the electrical topological state in terms of e.g. component outages with respect to a base case topology; 2) the *initial operating state* O describes the load, generation and import/export for the base case network topology.

We will assume a set of $|I| = n_{\text{os}}$ discrete initial operating states $(O_1, O_2, \ldots, O_{n_{\text{os}}})$. Each operating state i represents a certain number of hours during a year and has a duration denoted by Δt_i.

2.1.2. State vertices

A subset of the vertices of the graph $V_{\text{cont}} \subset V$ represents contingency states for the physical network (power grid), so that the vertex $v \in V_{\text{cont}}$ represents the contingency state C_v. We here understand a contingency as a failure or unplanned outage of one or multiple system components [40,53].

A sequence of events in the power system starts with an initiating event such as a primary failure [54] leading to a component being in a fault state. An initiating event is represented in the graph G by an initiating event vertex $v \in V_{\text{init}}$, where we have introduced $V_{\text{init}} \subseteq V_{\text{cont}}$ as the set of all vertices representing initiating events. Operating states with prior outages can be represented in the graph by separate initiating event vertices, and a simple implementation is described in more detail in 3.1.

Each initiating event vertex $v \in V_{\text{init}}$ is assigned a vector $\lambda_v = (\lambda_{v,1}, \lambda_{v,2}, \ldots, \lambda_{v,n_{\text{os}}})$ representing the frequency of occurrence for that type of initiating event. Here, $\lambda_{v,i}$ is the expected annual frequency of occurrence (i.e. failure rate) in initial operating state i, given that it lasted for the entire year. This representation can capture failure rates that vary in time (e.g. seasonally). To account for the fact that the operating state only lasts for a certain part of the year, we introduce a time-weighted failure rate

$$\lambda'_{v,i} = \frac{\Delta t_i}{\sum_{i \in I} \Delta t_i} \lambda_{v,i}. \tag{1}$$

In other words, $\lambda'_{v,i}$ is the expected number of that type of initiating event occurring per year while in initial operating state i.

2.1.3. Transition probabilities and transition mechanisms

Each edge $e = (v, v') \in E$ is assigned a weight for each initial operating state that is given by a vector of probabilities $\boldsymbol{p}_e = (p_{e,1}, p_{e,2}, \ldots, p_{e,n_{\text{os}}})$. Here, $p_{e,i} \in [0, 1]$ is the conditional probability of a sequence of events traversing edge e for initial operating state i:

$$p_{e,i} = \mathbb{P}(A_e \mid (C_v, O_i)). \tag{2}$$

Here we let $A_e = A_{(v,v')}$ denote the transition from the state represented by vertex v to the state represented by vertex v'. Eq. (2) implies that we model the event propagation as being Markovian, in conformity with most of related modelling approaches, cf. Section 1.1.

The framework has the flexibility to encode distinct probability values for each edge $e \in E$ and each initial operating state $i \in I$. However, transitions can typically be grouped to belong to a certain *transition mechanism*. Such mechanisms could be classified on the basis of e.g. [6–8]. We do not aim to propose a complete classification here, but mechanisms include: various protection and control system failures, failure of corrective actions (e.g. generation rescheduling, load shedding, grid reconfiguration), overload relays tripping (correctly or incorrectly), unintended system protection scheme interactions, generators losing synchronism and tripping, failure of islanding (e.g. due to frequency instability), etc. To exemplify the modelling of transition mechanisms in the framework, we consider the implementation of a selection of mechanisms in Section 3: Protection and control system failures (here: missing operation and unwanted unselective tripping), failure of generation rescheduling and load shedding (as examples of corrective actions), and failure of islanding.

In general, each transition mechanism is denoted by the index τ. In the lack of data justifying more detailed assumptions, we assume the same value $p = p_\tau$ for all edges representing the same mechanism τ. The method for analysing the uncertainty in these estimates p_τ will be described in Section 2.3.

2.1.4. Consequence vertices

For book-keeping reasons and to allow for a vulnerability analysis focusing on critical consequences, we introduce consequences as separate vertices $v^* \in V_{\text{cons}} \subset V$ in the graph G. The term consequence will in this article always refer to the consequence to the end-users of the power system, but the modelling framework is flexible with respect to how these consequences are defined and quantified.

A consequence vertex v^* represents the end point of some sequence of events, i.e. $\omega(P) = v^*$ for some (P, i). All consequence vertices v^* are joined to a contingency state vertex $v \in V_{\text{cont}}$ by an edge (v, v^*). This means that v^* represents the consequence of a sequence of events that reaches the contingency state C_v but does not propagate further.

All consequence vertices are associated with a numerical consequence value denoted by the general symbol Y. The consequence depends on the initial operating state, e.g. the amount of load at the delivery points that potentially can be lost. Therefore, a vector $\boldsymbol{Y}_{v^*} = (Y_{v^*,1}, Y_{v^*,2}, \ldots, Y_{v^*,n_{\text{os}}})$ is assigned to each contingency vertex v^*.

Depending on the implementation of the general methodology described here, the symbol Y could for instance represent the amount of interrupted power, the energy not supplied or the cost of energy not supplied. For the implementation presented in this article (cf. also Section 4.1), the term consequence will refer to the consequence of end-users in terms of the amount of interrupted power measured in MW.

2.2. Vulnerability analysis methodology

This section describes how the graph-based modelling framework can be used as a part of a quantitative vulnerability analysis. The purpose of the analysis is to identify critical sequences of events, vulnerabilities, and associated barriers to mitigate them. Given that a graph G describing possible sequences of events and their consequences has been constructed, the following subsections describe how it can be used to 1) identify sequences of events (i.e. paths in the graph) that

result in consequences, 2) estimate the likelihood of these events, 3) analyse critical sequences of events (for a given definition of "critical"), and 4) identify vulnerabilities and barriers.

2.2.1. Identify sequences of events

In the analysis that follows, we consider the sequences of events starting with some initiating event and ending in some power system consequence. For the sake of brevity, these sequences of events are in the following referred to simply as *events* when there is no ambiguity. To identify the sequences of events leading to a given consequence vertex $v^* \in V_{\text{cons}}$ we first identify the set of paths

$$S_P^{v^*} = \{P \in S_P \mid \alpha(P) \in V_{\text{init}} \ \wedge \ \omega(P) = v^*\} \subseteq S_P. \tag{3}$$

Each of these events (P, i) are associated with a measure of the consequence, given by

$$Y_{P,i} = Y_{v^*=\omega(P),i}. \tag{4}$$

2.2.2. Estimate likelihood of events

The information encoded in G can be used to estimate the expected annual frequency of occurrence $\lambda_{P,i}$ of an event (P, i). For brevity, $\lambda_{P,i}$ will be referred to as a measure of the *likelihood* of the event (following the usage of the term in [50]). Using information about the failure rate for initiating events $\lambda_{v,i}$ and the conditional transition probabilities $p_{e,i}$, the likelihood of (P, i) can be estimated as

$$\lambda_{P,i} = \lambda'_{v,i} \prod_{e \in P} p_{e,i}. \tag{5}$$

Here, Eq. (1) has been used to calculate the time-weighted failure rate $\lambda'_{v,i}$.

The risk of each event (P, i) is quantified by the combination of its estimated consequence and likelihood, i.e. the pair $(Y_{P,i}, \lambda_{P,i})$. By plotting the identified events along these two risk dimensions one can visualize the risk in the form of a risk diagram.

2.2.3. Identify critical sequences of events

We follow an approach to vulnerability analysis that focuses on the consequence dimension of risk and in particular on events with critical consequences [4,10]. The modelling framework is flexible with respect to how the threshold for criticality is defined. Here, for the general consequence measure Y, we simply let $Y \geqslant Y_{\text{crit}}$ define a critical consequence. For vulnerability analysis of real systems, the value of Y_{crit} should be defined prior to the analysis together with relevant stakeholders and decision makers [10,11].

Given the graph G and the threshold Y_{crit}, the set of critical consequence vertices $V_{\text{cons}}^{\text{crit}} \subseteq V_{\text{cons}}$ can formally be defined as follows:

$$V_{\text{cons}}^{\text{crit}} = \{v^* \in V_{\text{cons}} \mid Y_{v^*,i} \geqslant Y_{\text{crit}} \text{ for some } i \in I\}. \tag{6}$$

We define a *critical path* as a path that leads to a critical consequence for at least one initial operating state. Mathematically, the set of critical paths S_P^{crit} can be expressed as

$$S_P^{\text{crit}} = \{P \in S_P^{\text{events}} \mid \omega(P) \in V_{\text{cons}}^{\text{crit}}\} \subseteq S_P. \tag{7}$$

A *critical sequence of events* is defined by a pair $(P, i) \in S_P^{\text{crit}} \times I$ for which $\lambda_{P,i} > 0$. The critical events are identified by first using Eq. (6) to find the critical consequence vertices $V_{\text{cons}}^{\text{crit}}$ and then using Eq. (7) to find the critical paths S_P^{crit} leading to this vertices. (See also the illustration for step 3 in Fig. 1.)

2.2.4. Identify vulnerabilities and barriers

One can gain understanding into critical sequences of events and insight into associated vulnerabilities by analysing the critical paths S_P^{crit}. This can be done by extracting subgraphs of S_P^{crit} for selected consequence vertices using Eq. (3) and visually inspecting the paths leading to this consequence vertex.

From considering the edges $e \in P$ for $P \in S_P^{\text{crit}}$ one can find which transition mechanisms are involved in critical sequences of events and thus which barriers need to fail for it to occur. This can be quantified by identifying the set of paths $S_P^{\text{crit},\tau} \subseteq S_P^{\text{crit}}$ that contain edges for transition mechanism τ and calculate the number of possible sequences of events corresponding to these paths:

$$\sum_{P \in S_P^{\text{crit},\tau}} \sum_{i \in I} |\{i \in I \mid \lambda_{P,i} > 0\}|. \tag{8}$$

Similar calculations can also be carried out for the number of critical sequences of events where the initiating event involves a certain power system component k, i.e. for which $k \in C_v$ for $v = \alpha(P)$.

The quantitative results and insights obtained by this methodology can then be used to inform decisions about which vulnerability-mitigating measures to prioritize and which barriers to strengthen. These considerations can be complemented by uncertainty analysis results described in Section 2.3 and by more qualitative vulnerability assessment as described in [9,10]. Application of the methodology is exemplified and demonstrated in Section 4.3.

2.3. Uncertainty analysis

This section describes the method adopted for quantifying the uncertainties in the results of the vulnerability analysis presented in Section 2.2. More specifically, we consider the estimate of the likelihood measure $\lambda_{P,i}$ for event (P, i) as calculated by Eq. (5). In the following we suppress the subscripts of $\lambda_{P,i}$ to simplify notation and express it as a general function $\lambda = f(\boldsymbol{x})$ of uncertain input parameters $\boldsymbol{x} = \{x_1, x_2, ..., x_N\} \in \mathbb{R}^N$.

The aim of the uncertainty analysis is to quantify the implications of uncertainties in $\boldsymbol{x}$ on uncertainties in $\lambda = f(\boldsymbol{x})$. In our case, the uncertain input parameters could be the set of conditional probabilities for the transition mechanisms, i.e. $x_i = p_\tau$ for transition mechanism τ. (Concrete examples are given in Section 3.) The advantage of the proposed approach is that the graph G does not need to be re-constructed for each realization of uncertain input parameters $\boldsymbol{x}$ that is considered. Instead, for each iteration it is sufficient to re-assign the weights p_e of an appropriate subset of the edges e in G before re-calculating $\lambda_{P,i}$.

In our case the input parameters in $\boldsymbol{x}$ are associated with so-called epistemic uncertainty, i.e. uncertainty due to a lack of knowledge [50]. There are little data available to describe the uncertainty in these conditional probabilities, and one may not justify specifying a probability density function that describes the probability of different values of the uncertain parameters. However, we can still specify our assumptions about which values of the uncertain parameters are possible and then analyse the implications of these assumptions. In the following, we therefore propose using possibilistic uncertainty analysis techniques. For more details on related methods for handling epistemic uncertainties we can refer e.g. to [50,51]. We also note that some elements of aleatory uncertainty, associated with natural variability rather than a lack of knowledge, are already captured in the proposed framework: The conditional probabilities p_e represent the uncertainty in which sequence of events follows after a given realization of an initiating event, and variability in e.g. load and failure rates is captured by considering multiple initial operating states.

A possibilistic uncertainty representation for a quantity is based on a possibility distribution $\pi(x)$ representing the degree of possibility (not probability) of the parameter x. The function $\pi(x)$ by definition fulfills $0 \leqslant \pi(x) \leqslant 1$; if $\pi(x) = 0$ for a value of x, this means that this value is impossible. We adopt the α-cuts technique [50], where a so-called α-cut for a general uncertain variable $\boldsymbol{x}$ is defined as

$$A_\alpha = [x_\alpha^-, x_\alpha^+] = \{x \in \mathbb{R} \mid \pi(x) \geqslant \alpha\}. \tag{9}$$

For each input parameter x_i in $\boldsymbol{x}$ we construct M α-cuts from the possibility distributions $\pi(x_i)$ for the parameter. These α-cuts will be denoted A_{x_i,α_j} and calculated for the set of α values $\{\alpha_1, ..., \alpha_M\}$ using Eq. (9). We then let $\boldsymbol{A}_{\alpha_j} \in \mathbb{R}^N$ denote the hyper-rectangle formed by the jth

α-cut for the N individual variables in $\boldsymbol{x}$ [51]:

$$\boldsymbol{A}_{\alpha_j} = A_{x_1,\alpha_j} \times \cdots \times A_{x_N,\alpha_j} = \{\boldsymbol{x} \mid x_1 \in A_{x_1,\alpha_j} \bigwedge \ldots \bigwedge x_N \in A_{x_N,\alpha_j}\}. \quad (10)$$

To propagate the uncertainties in the input parameters $x_1, \ldots, x_N$ through the function f to the resulting uncertainty in λ, we calculate M α-cuts $A_{\lambda,\alpha_j} = [\lambda^-_{\alpha_j}, \lambda^+_{\alpha_j}]$ for λ for each $\alpha_j \in \{\alpha_1, \ldots, \alpha_M\}$ as follows:

$$[\lambda^-_{\alpha_j}, \lambda^+_{\alpha_j}] = [\min_{\boldsymbol{x} \in \boldsymbol{A}_{\alpha_j}} f(\boldsymbol{x}), \max_{\boldsymbol{x} \in \boldsymbol{A}_{\alpha_j}} f(\boldsymbol{x})]. \quad (11)$$

The possibility distribution $\pi(\lambda)$ is then constructed from this set of α-cuts for the output parameter λ. When the function $f(\boldsymbol{x})$ depends monotonically on its input parameters x_i it is sufficient to evaluate the vertices of the hyper-rectangles $\boldsymbol{A}_{\alpha_j}$ when searching for the function extrema in Eq. (11). This will be the case for the path frequencies defined in Eq. (5) for the implementation considered in this article.

3. Exemplary implementation of the modelling framework

This section describes a concrete implementation that exemplifies the graph-based modelling framework by introducing basic models for three selected examples of transition mechanisms: i) protection and control system failures (Section 3.2), ii) failure of corrective actions (generation rescheduling and controlled load shedding, Section 3.3), and iii) failure of islanding (Section 3.4). The implementation also includes modelling of prior outages that can lead to contingency states due to independent multiple-outage occurrences [55] (overlapping outages). This does not represent a transition mechanism *per se*, but a prior outage can nevertheless be seen as a vulnerability of the system and can thus be important to consider on an equal footing with the transition mechanisms. We therefore begin by briefly stating the modelling assumptions for prior outages in Section 3.1.

3.1. Prior outages

For illustration we consider the case of a prior unplanned outage of component k_1. (Prior planned outages could also be considered in the general framework.) The state with a fault on component component k_2 while component k_1 is in the outage state is denoted $C_v = \{k_1, k_2^*\}$. (See Figs. 7 and 10 below for examples.) A simplified expression for the frequency of occurrence of this initiating event while in initial operating state i is [40]

$$\lambda_v = \mathbb{P}(\{k_1\} \mid O_i) \cdot \lambda_{k_2,i} = \frac{\lambda_{k_1,i}\lambda_{k_2,i}}{\lambda_{k_1,i} + \mu_{k_1}}. \quad (12)$$

Here $\mathbb{P}(\{k_1\} \mid O_i)$ is the probability of component k_1 being in an outage state given initial operating state i, and μ_k is the repair rate of component k. In anticipation of the case described in Section 4, with seasonal time dependence of failure rates , we have made the simplifying assumption that each prior outage event is contained within a single operating state. In the model we furthermore make the assumption that the sequence of events propagates so rapidly that one can neglect the possibility of an independent primary failure occurring during the sequence.

3.2. Protection and control system failures

The purpose of power system protection is to clear faults and minimize the damage they cause. However, unintended actions of protection systems may sometime aggravate the damage and lead to multiple outages and severe consequences. In fact, missing, unsuccessful or unintended actions of protection and control systems is an important contributor to power interruptions in general [56] and major blackouts in particular [1,37]. The successful operation of protection systems can thus be considered as a barrier that prevents a failure event from propagating.

In this implementation, we consider models for two types of failures

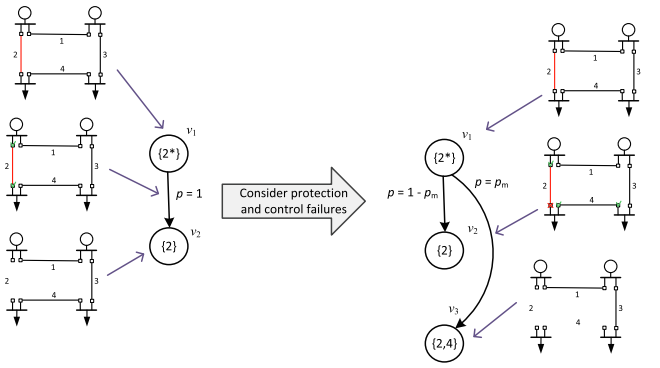

Fig. 4. Illustration of graph construction representing protection and control system failures (missing operation).

of such a barrier: 1) *Missing operation*: Primary failure of primary equipment combined with fault in circuit breaker or secondary equipment, leading to missing operation of circuit breaker. 2) *Unwanted unselective tripping*: Primary failure of primary equipment combined with fault in circuit breaker protection system, leading to unwanted unselective tripping of circuit breaker. The definition and modelling of these protection system failure scenarios builds upon previous work done in the context of analytical power system reliability analysis [40,41,57].

The model for missing operation as a transition mechanism associates a conditional probability p_m to a transition from a fault state for a branch to the contingency state where this and a neighbouring branch are in an outage state. The right-hand side of Fig. 4 illustrates how the construction of the graph proceeds when considering this transition mechanism for a simple 4-bus test system. In this example, branch 2 is initially in a fault state, indicated by a red colour for the branch in the single-line diagram. This contingency state is denoted {2*} and associated with vertex v_1. (The left-hand side of Fig. 4 illustrates the sequence of events without considering protection and control system failures.) From the state $C_{v_1} = \{2^*\}$ two things can happen: i) The system can either transition to the outage state $C_{v_2} = \{2\}$ if the protection system clears the fault correctly (here with probability $p = 1 - p_m$), or ii) it can transition to the contingency state $C_{v_3} = \{2, 4\}$ if the fault at branch 2 has to be cleared by back-up protection systems due to missing protection system operation ($p = p_m$) which causes the additional outage occurrence of branch 4. Both these cases are presented in one graph on the right hand side of Fig. 4.

The model for unwanted unselective tripping as a transition mechanism associates a conditional probability p_u to the transition from an outage state for a branch to the contingency state where an additional, neighbouring branch are in an outage state. Fig. 5 illustrates how the construction of the graph proceeds when considering this transition mechanism. After the system has transitioned from $C_{v_1} = \{2^*\}$ to $C_{v_2} = \{2\}$, where the protection system has cleared the primary fault as intended, the system may transition further to $C_{v_3} = \{2, 4\}$ with probability $p = p_u$ due to the unintended action of the protection system for the neighbouring branch 4.

3.3. Failure of corrective actions (generation rescheduling and controlled load shedding)

When estimating the consequence Y associated with a contingency state C_v one needs to make some assumptions about the system response and corrective actions taken by the system operator [45]. These actions may include e.g. generation rescheduling, grid reconfiguration, generation rejection and load shedding [44,45,58]. Typically, corrective action models will assume that the corrective actions are successfully operated and that afterwards, any operational security limit violations following from the contingency will have been alleviated. However,

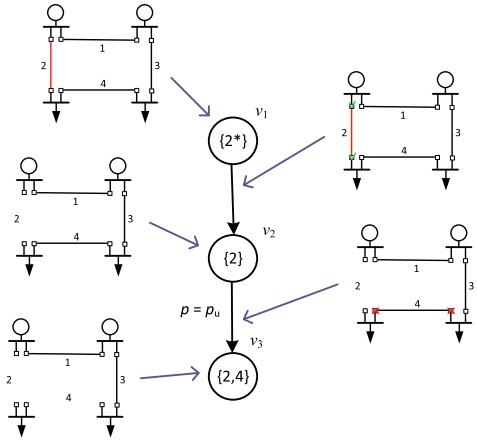

Fig. 5. Illustration of graph construction representing protection and control system failures (unwanted unselective tripping).

corrective actions may fail to operate successfully. This failure of corrective actions may cause the system to transition from the state C_v to another state $C_{v'}$ (e.g. where additional branches are in the outage state) for which consequences may be more severe. There is currently a lack of data on corrective action failures [44], and only a few research works [46,47] are published that explicitly models the possibility of failure of corrective actions.

Adopting some of the formalism of [44], we can denote the event that corrective actions fail to operate (i.e. missing operation) by X_c. The conditional probability that the corrective actions fail to operate given that a contingency C_v has occurred during initial operating state i is then given by $\mathbb{P}(X_c \mid (C_v, O_i))$. Here we will assume that X_c and C_v are independent events so that the probability of corrective action failure is

$$\mathbb{P}(X_c \mid (C_v, O_i)) = \mathbb{P}(X_c) \equiv p_c \tag{13}$$

For this implementation, we focus on generation rescheduling and controlled load shedding as corrective actions for alleviating an overloaded branch. We consider a simple model where the failure of these corrective actions leading to tripping of the overloaded branch. The modelled transition mechanism is illustrated in Fig. 6. For each contingency state C_v an AC power flow calculation is carried out to check for branch overloads for each initial operating state i. If for any i a branch k is overloaded, and corrective actions thus would be needed to alleviate this overload, an auxiliary contingency state $C_{v'}$ is added to

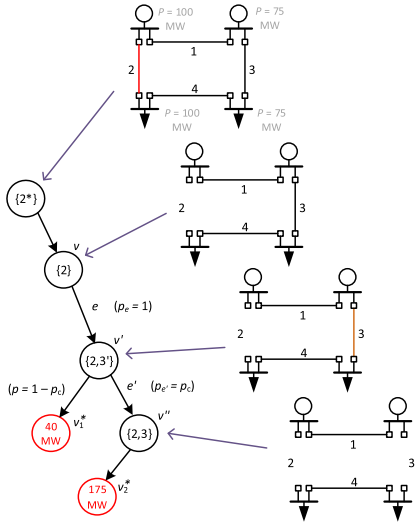

Fig. 6. Illustration of graph construction representing failure of corrective actions.

represent a state with the same topology as C_v but with overload on branch k. In the example in Fig. 6, $C_v = \{2\}$, and we have denoted the auxiliary contingency state by $C_{v'} = \{2, 3'\}$, where the overloaded branch $k = 3$ is indicated by an orange colour in the single-line diagram. (Branches are assumed to have 135 MW power transmission capacity in this example, and load and generation is indicated in the topmost single-line diagram in Fig. 6.)

In the model, the edge $e = (v, v')$ is added to join the states. This edge is assigned a conditional probability $p_{e,i} = 1$ for those operating states i where overloading occurred and $p_{e,i} = 0$ for those where it did not.

Another edge $e' = (v', v'')$ assigned the conditional probability $p_{e',i} = p_c$ is added to join the overload state $C_{v'}$ and the contingency state where the branch k has been tripped due to the failure of corrective actions. In the example in Fig. 6, $C_{v''} = \{2, 3\}$, and the failure of corrective actions leads to the loss of all load in the system ($Y = 175$ MW). If on the other hand corrective actions are successful, controlled shedding of some of the load will alleviate the branch overload ($Y = 40$ MW). Consequence vertices $v^* \in V_{cons}$ are shown in red.

In this exemplary implementation, e' generically represents a mechanism that leads to the tripping of the overloaded branch after failure of generation rescheduling and/or controlled load shedding. In practice such tripping could occur due to delays to the corrective actions being effectuated, e.g. due to lack of situational awareness, or due to human (operator) error (e.g. for manual generation rescheduling) or computer or communication error (for automatic generation rescheduling) [6–8].

According to this model, the possibility of corrective action failures is not relevant for those operating states (C_v, O_i) where the power flow calculation do not result in branch overloads. For these operating states, the consequence is therefore assumed to be zero. For book-keeping purposes, a consequence vertex with $Y = 0$ MW is thus added if this is the case for any i. This consequence vertex with zero consequence is joined to the contingency state vertex C_v by an edge e'' with $p_{e'',i} = 1$ for those i where no overloads occur. (Not shown for the initial operating state considered in Fig. 6).

3.4. Failure of islanding

An island is defined as a portion of a power system that is disconnected from the remainder of the system but remains energized [59]. Failure of islanding is here used to describe a general mechanism whereby generators are tripped in a (potential) island after (unintentional) system separation. To avoid the consequences of such an event, system operation must remain stable for each island and the islands have to be able to operate separately (in island mode). In a real power system, the success or failure of islanding depends on a number of factors, such as the load/generation imbalance (i.e. the operating state) in the island prior to the contingency and the dynamic characteristics of the island [1,3,49].

In the spirit of the general approach presented in the preceding sections, we will in the current implementation forego detailed dynamic simulations for the following simplifying and transparent model: A probability p_i is assigned to the failure of the island that does not contain the swing bus. The island with the swing bus is on the other hand assumed to always survive islanding [45]. This assumption is justified when the concept of a swing bus makes physical sense [60], that is, when the swing bus represents a bus with large generation units capable of controlling the system frequency and supporting island mode. One should however be aware that this assumption does not hold true generally.

The model for this transition mechanism represents the network topology as a graph $G_{network}$. When evaluating each contingency state vertex v for possible transition mechanisms and consequences, one identifies whether $G_{network}$ is disconnected and contains several graph components [52] (i.e. potential islands) each having generators and delivery points. Fig. 7 shows an example where a failure occurs at

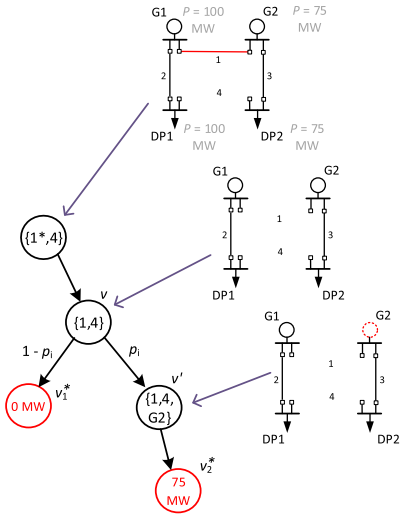

Fig. 7. Illustration of graph construction representing the failure of islanding.

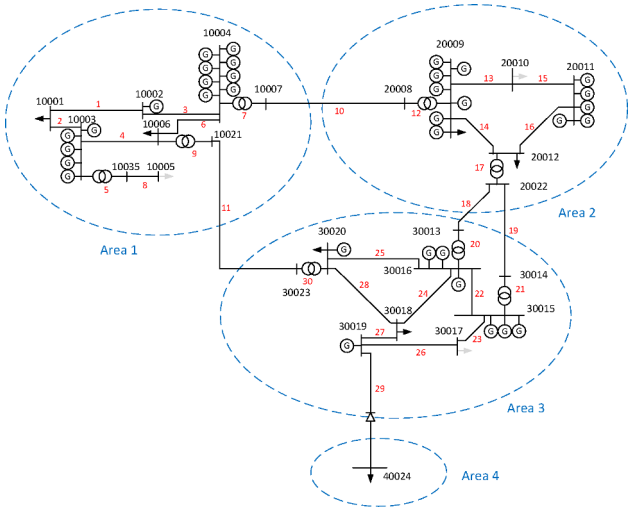

Fig. 8. Test network considered in the case study (based on [63]).

branch 1 during a prior outage of branch 4. In the resulting contingency state $C_v = \{1, 4\}$, the network separates into two islands: one including the swing bus to which generator 1 is connected, and the other including generator 2. As illustrated in Fig. 7, there is a probability p_i that islanding will fail for the island with generator 2 and that the system thus transitions to state $C_{v'} = \{1, 4, G2\}$ in which generator G2 is tripped. In this state, there is no generation to supply the load in the island (75 MW), and the load is lost (consequence vertex v_2^*). On the other hand, there is a probability $1 - p_i$ that islanding succeeds for both islands and that there is no load lost (consequence vertex v_1^*).

4. Case study

In this section we illustrate the application of the vulnerability analysis framework considering the exemplary implementation described in Section 3. Details on the software implementation of the modelling framework are given in Section 4.1, and the test system considered is described in Section 4.2. Results of the case study are presented and discussed in Section 4.3.

4.1. Software implementation

The modelling framework is implemented using the Python library *graph-tool* [61] for constructing and analysing the graph G. To estimate consequences of contingency states and represent the possibility of corrective action failures, the implementation is interfaced with the consequence analysis models described in [45,57]. These models offer a set of options for quasi-static simulations of the system response to contingencies and use MATPOWER [62] for AC power flow calculations. Lost load Y for consequence vertices are evaluated by an AC optimal power flow model for generation rescheduling and load shedding [45], representing successful operation of corrective actions. Failure of corrective actions to alleviate branch overloads is represented by running an AC power flow calculation and tripping of the most overloaded branch [45].

4.2. Test system and case set-up

The network model considered for the case study is a 25-bus test system that represents a power system with four distinct areas. The single-line diagram for the model is shown in Fig. 8. This test system represents small regions of the Nordic power system, and it has been developed and used for integrated power market and reliability analyses [45,57,63]. In this case study we use a variant of the network that has additional branches and thus is relatively reliable; this is the same variant as used in [45]. Branch impedances and other data for static power flow analysis are available online [64]. Failure rates and outage times for the branches are also included with the data set. The branch numbers are given in red labels in Fig. 8. The swing bus is bus 30019.

The case study includes 12 operating states, where each operating state represents 10 a.m. on a Monday for all months in a year. (Operating state data are also available online [64].) These operating states are based on representative time dependence of load demand in the Norwegian power system. Data for the time-dependence of failure rates are based on the Norwegian standardised system FASIT for collection, calculation and reporting of disturbance and reliability data [65] and implemented according to the methodology described in [40,57,66].

We include the transition mechanisms τ described in Section 3, and these are listed in Table 1 together with their conditional probabilities p_τ. The probabilities for protection system failure (p_u and p_m) are based on the assumptions used in [41]. The values for the probabilities for failure of corrective actions and islanding (p_c and p_i) are simply chosen to be somewhat smaller than those for protection system failure. This choice is made for the purpose of illustration in the absence of data [44]. However, the lack of data is represented in the uncertainties assigned to the probabilities, which are also specified in Table 1. For simplicity we choose a triangular possibility distribution $\pi(p_\tau)$, where $[p_{\tau,-}, p_{\tau,+}]$ is the interval of values that are considered possible ($\pi(p_\tau) > 0$), and $\pi(p_{\tau,0}) = 1$ for the value $p_{\tau,0}$ that is our "best guess" for the value of p_τ. In practical applications of the methodology, the values of these parameters can be assigned through an expert elicitation process with power system operator or other stakeholders.

4.3. Results

The software implementation described in Section 4.1 is used to construct the graph G for the case described in Section 4.2. The full graph G is not shown here since it is too large to visualize in a way that provides any insight. It is however formed by state transitions as illustrated in Section 3, including failures of power system components, clearing of faults, protection system failures, overloading, failure of corrective actions, and failure of islanding. Results in the form of subgraphs of G that serve to visualize critical sequences of events and provide insights into the vulnerability of the system are shown in Section 4.3.2.

Results obtained from G are first presented in the form of risk diagrams, first considering a single operating state in Section 4.3.1 and then multiple operating states in Section 4.3.3. The methodology also allows for visualizing the uncertainties associated with the likelihood

Table 1
Conditional probabilities p_τ with uncertainty representation assumed for the case study for transition mechanisms τ.

Transition mechanism	Best-guess probability $p_{\tau,0}$	Lower probability $p_{\tau,-}$	Upper probability $p_{\tau,+}$
Missing protection system operation (p_m)	0.0205	0.01	0.04
Unwanted unselective tripping (p_u)	0.007	0.004	0.02
Failure of corrective actions (p_c)	0.02	0.005	0.04
Failure of islanding (p_i)	0.01	0.002	0.04

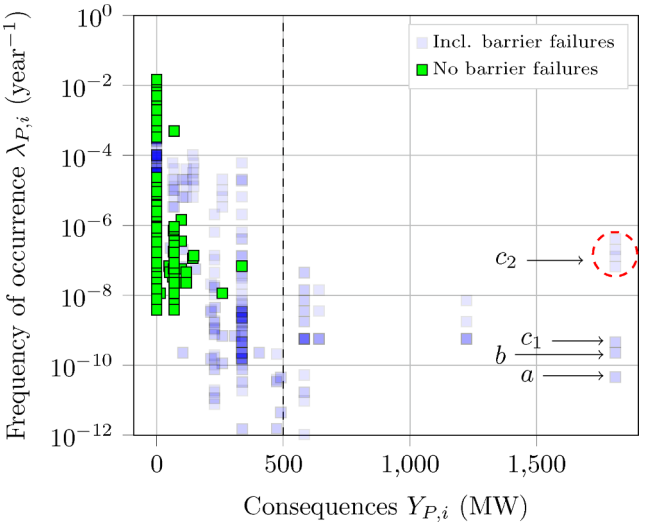

Fig. 9. Risk diagram with sequences of events with and without considering barrier failures, including only results for a single operating state ($i = 1$).

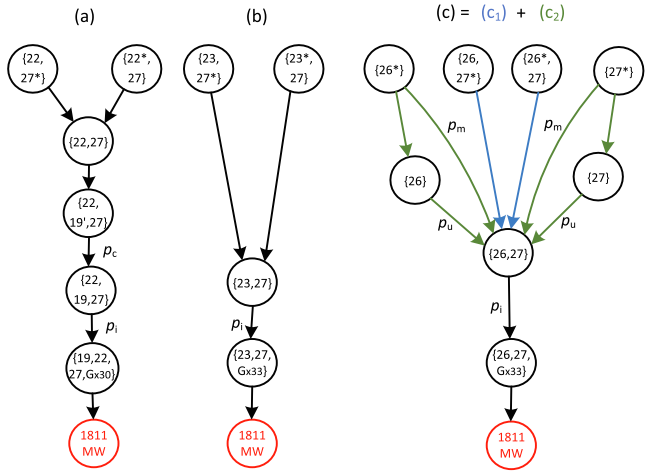

Fig. 10. Graphical representation of the paths for the most critical sequences of events shown in Fig. 9. G × 30 denotes all generators except those at buses 30016 and 30019 (30 generators), and G × 33 denotes all generators except that at bus 30019 (33 generators).

dimension, but for the purpose of clarity, uncertainty estimates are not included until Section 4.3.5. Section 4.3.4 analyses vulnerabilities by considering all the identified critical sequences of events.

4.3.1. Identifying sequences of events (one operating state)

To illustrate the benefits of the proposed approach, we first compare the results of our methodology with results from a more conventional contingency analysis. In the risk diagram in Fig. 9, the green data points are obtained using our methodology but neglecting the possibility of barrier failures, i.e. setting $p_m = p_u = p_c = p_i = 0$. Each data point in the risk diagram corresponds to an event (P, i). For clarity, only results for a single operating state ($i = 1$, which is in January) has been included here.

The results without barrier failures in Fig. 9 (green) can be compared with the blue data points. These results are obtained assuming the conditional probabilities of barrier failures given in Table 1. The possibility of prior outages is included for both sets of results.

Comparing the two sets of results in Fig. 9 one observes that accounting for barrier failures introduces new events in the risk diagram with higher consequences and higher likelihoods. Because there are many events with similar consequence and likelihood estimates, the blue data points are drawn partly transparent to better see the density of events in the risk diagram. The criticality threshold chosen for this case study ($Y_{crit} = 500$MW) is shown as a dashed line in the figure. This figure illustrates the advantage of implementing several transition mechanisms in the modelling framework: It can be seen how including the possibility of barrier failure in this case is essential to be able to identify events with critical consequences.

The results accounting for barrier failures also reveal the possibility of events with very severe consequences (1811 MW lost load) at the far right-hand side of Fig. 9. These groups of events are labeled in the figure for later reference. Although the events are associated with low likelihoods of occurring, the estimated likelihoods are higher than for many of the events with lower consequences.

4.3.2. Understanding critical sequences of events

We next inspect the results underlying in Fig. 9 more closely to gain insight into sequences of events that may lead to critical consequences. We focus on the events (a), (b), (c_1) and (c_2) in Fig. 9 ($Y = 1811$ MW), and Fig. 10 depicts the critical paths corresponding to these events. These paths were obtained by first searching for the critical consequence vertices v^* and then searching for the set of paths $S_P^{v^*}$ using Eq. (3). In this case, $S_P^{v^*}$ comprises three disconnected subgraphs of G and three such critical consequence vertices v^*. Each of these subgraphs can be regarded as a fault tree describing different sequences of events through which a given critical consequence might come about. One can note that all the sequences of events in Fig. 10 involve the failure of islanding, i.e. the paths include an edge with weight p_i.

In subgraph (a) in Fig. 10, the overlapping outage of branches 22 and 27 leads to branch 19 (which is parallel to 22) being overloaded. Tripping of branch 19 would then lead to generators at bus 30015 and 30019 (which amount to over 20% of the generation capacity in the system) to be separated from the rest of the system. Failure of the rest of the system to survive the system separating into an upper and a lower part would could then cause a loss of 1811 MW of load. This can be regarded as an extreme scenario, but then the estimated likelihoods associated with these events are also extremely low: around $\lambda_{P,i} = 4.6 \times 10^{-11}$ year^{-1} for $i = 1$. The reason is that these events require a prior outage, corrective action failure *and* the failure of islanding to occur.

As mentioned in Section 3.4, the likelihood of failure of islanding in practice depends on several factors, including the generation/load imbalance and the capabilities of the individual power plants involved. Considering such factors in more detailed simulations could therefore be a natural next step after identifying potentially critical events. A subsequent and more detailed analysis of the event could then be carried out to improve the preliminary estimate of the likelihood. It might for instance uncover that for this particular event, with the upper part of the system (areas 1 and 2 and most of area 3) containing many large

generation units, the failure probability p_i would be even lower than the general assumption in Table 1.

We next consider the subgraphs (b) and (c) in Fig. 10, where only the generator at bus 30019 is isolated from the rest of the system. In comparison with the situation in the leftmost subgraph, this situation can occur through a larger number of paths, and the estimated likelihoods are higher. For instance, the sequence (P, i) initiated by a failure of branch 27 and followed by missing protection system operation (p_m) and subsequent tripping of branch 26 has $\lambda_{P,i} = 4.1 \times 10^{-7}$ year^{-1} for $i = 1$. The four paths (c_2) in Fig. 10 that have edges with weights p_m or p_u correspond to the four events labelled (c_2) in Fig. 9. These four events have much higher likelihood than the events in Fig. 9 corresponding to paths in (a), (b) or (c_1). The reason is that in contrast to the other paths in Fig. 10, c_2) involve protection system failures. In other words, because branches 26 and 27 are adjacent, the consequence vertex corresponding to this critical consequence in Fig. 10 is not dependent upon prior outages to be reached. The system therefore has a vulnerability with respect to these sequences of events involving protection system failures. A possible barrier that could be put in place to mitigate this vulnerability could be to pay extra attention to protection system settings for branches 26 and 27.

4.3.3. Identifying sequences of events (multiple operating states)

The results above were only considered for a single operating state ($i = 1$), and we now consider results for all $n_{os} = 12$ operating states. The resulting risk diagram is shown in Fig. 11. There are in total 2187 events with non-zero consequences shown in the risk diagram in Fig. 11, and these events are described by 534 distinct paths in the graph G.

It can be observed from Fig. 11 that events represented by (c_2) in Fig. 10 can be found for all operating states i. The consequences of these events are lower for $i > 1$ than for $i = 1$ (shown in Fig. 9) because the load demand are lower for $i > 1$ than for $i = 1$. Events corresponding to the paths (a), (b) and (c_2) are also possible for other operating states than $i = 1$. These are found in Fig. 11, below (c_2) in the risk diagram. However, in contrast to (c_2), not all of these events are found for all operating states $i > 1$. The reason is that branch 19 cannot be overloaded in operating states with significantly lower system load, and the edge e corresponding to overloading in the paths (a) therefore has $p_{e,i} = 0$ for these operating states. Or simply put, the paths are not possible sequences of events for all operating states.

4.3.4. Identifying vulnerabilities

Using the methods in Section 2.2.3, we find that 412 of the 2187 events in Fig. 11 lead to consequences regarded as critical. The identified events include all the events that are critical for this particular case and given the transition mechanism models that are implemented. Eq. (8) tells us that almost all (404 out of the 412) critical events involve failure of islanding. Branch tripping due to overload and failure of corrective actions is on the other hand involved in a much smaller proportion of the critical events (64 out of 412). The same proportion of the critical events involve protection system failure.

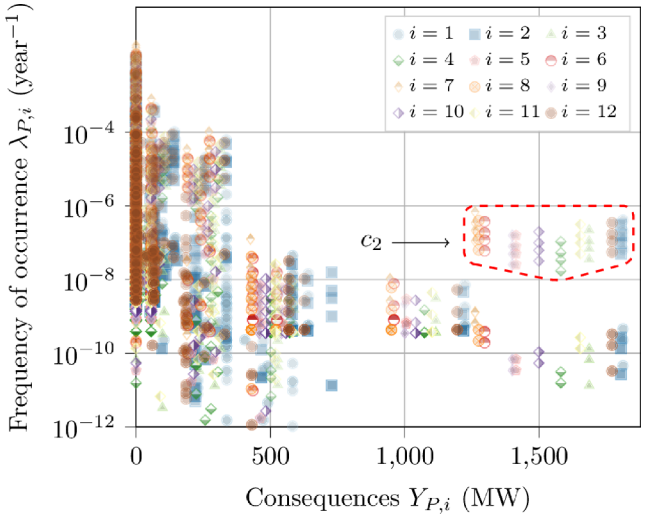

Fig. 11. Risk diagram with all sequences of events for all operating states.

As mentioned in Section 1.1, previous work [27] has found that the set of power system components typically outaged in the initiating events is not necessarily similar to the set of components outaged during the subsequent sequences of events. We can confirm this for our case by considering the edges e and initiating event vertices v as described in Section 2.2.4. For instance, we find that branches 26 and 27 are among the components most commonly involved in initiating events (for 80 and 48 events, respectively). On the other hand, branches that are involved in critical events in the sense of being tripped due to corrective action failures include 11 and 30 (in 26 and 18 events, respectively). These are branches which connect area 1 with area 3. A relevant barrier to mitigate this vulnerability could therefore be to increase the power transfer capacity between area 1 and 3. However, vulnerability-mitigating measures aiming to reduce branch failure rates should rather prioritize branches 26 and 27.

The results above allow us to make the following conclusions, given the assumptions in the case, about the vulnerabilities of the system: 1) Protection system failures are important to take into account. 2) The system is not particularly vulnerable to failure to alleviate branch overloads due to corrective actions failure, and the main reason is that the system is relatively strongly meshed. 3) Still, failure of islanding remains as a potential vulnerability in the system. The system is made up by several large areas that both contain generation and load, and generation and load is evenly distributed throughout the system. Thus there are few sequences of events through which load and generation buses can be separated or large generation deficits can be formed in parts of the system. Large-scale load shedding is therefore dependent on generators to trip for other reasons. Thus, ensuring that the areas in the system are able to operate as islands is important to mitigate critical consequences. Whether one estimates such consequences to be likely will however depend on the model implemented for failure of islanding. Therefore, for real applications, such potential vulnerabilities should be subsequently scrutinized using more detailed models.

Note that the conclusions above are specific to the power system model considered in the case study and follow from the characteristics of that system. The methodology is general, however, and applied to other power system models it could reveal other conclusions about the vulnerabilities of those systems.

4.3.5. Uncertainty of sequences of events

In Fig. 12 we focus on the critical sequences of events ($Y > Y_{crit} = 500$MW) and also include error bars representing the uncertainty in the estimated $\lambda_{P,i}$. More specifically, the error bars cover the range of values considered possible ($\alpha = 0$) according to the possibilistic uncertainty analysis of Eq. (11). One can observe that the uncertainty associated with the events is very large (of the same order of magnitude as $\lambda_{P,i}$ itself), as they all are dependent upon one or more barrier failures that each have substantial uncertainty. One can nevertheless conclude with certainty, given the assumptions in Table 1, that the likelihoods of the four paths (c_2) involving protection system failure in Fig. 10 are higher than the likelihood of the paths in (a), (b) and (c_1). Such findings can be helpful in decision making: For a set of identified events with the same critical consequence, one can prioritize to strengthen barriers against those events one knows are certainly more likely. In this case, that could mean that one should prioritize testing protection system settings for branches 26 and 27.

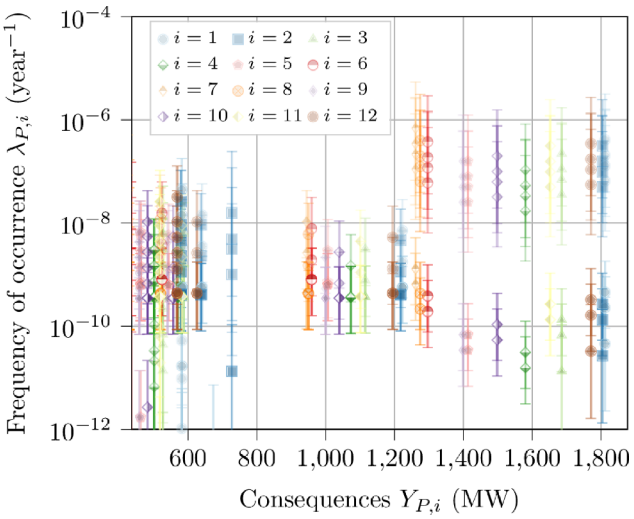

Fig. 12. Risk diagram with sequences of events leading to critical consequences (for the consequence threshold Y_{crit} = 500MW) for all operating states.

5. Conclusions and further work

In this article we have presented a vulnerability analysis methodology based on a general modelling framework for describing sequences of events leading to power supply interruptions. In summary, the advantages of this approach that have been demonstrated in this article are that i) the vulnerability analysis can be used to identify critical sequences of events and barriers, ii) the graph-based representation allows for exploring sequences of events and understanding vulnerabilities, iii) the modelling framework is general and can incorporate multiple transition mechanisms, and iv) the analysis accounts for the large uncertainty associated with critical sequences of events. In concluding the article we will elaborate on each of these contributions and suggest some directions for further work.

i) Vulnerability analysis: The uniqueness of the framework lies in how it structures information about the relationship between events, barriers and consequences in a graph representation that allows it to be used for vulnerability analysis. We showed how this can be used to identify potential critical sequences of events, vulnerabilities in the system, and barriers to mitigate them. The case study findings (summarized in Section 4.3.4) illustrated the insights that the methodology could provide into the significance of different vulnerabilities. The vulnerability analysis methodology is general, but such findings and insights are likely to be specific to each power system that is analysed. Our approach to vulnerability analysis considers both the consequence and likelihood dimension of risk: It focuses on the potential critical consequences but also provides estimates of their likelihood.

ii) Exploring sequences of events: We showed how using a graph-based description makes it easier to explore and understand the sequences of events. After the graph has been constructed, fault trees or individual critical paths can be extracted and visualized as sub-graphs (as demonstrated in Section 4.3.2) to better understand vulnerabilities and how critical consequence might come about. This approach can be contrasted with conventional contingency analyses, which often take a given contingency (combination of overlapping component outages) as a starting point without considering how that contingency might arise.

iii) Generality: This article also presented a concrete implementation of the modelling framework including exemplary models for protection system failures, failure of corrective actions (generation rescheduling and controlled load shedding), and failure of islanding. The modelling framework presented in Section 2 is however general and not restricted to these mechanisms. The exemplary models in Section 3 and the case study in Section 4 demonstrates that the modelling framework allows multiple mechanisms to be implemented. This means that the vulnerability analysis to a greater extent than existing methods can reveal the relative significance of different mechanisms.

One natural extension of this work could be to implement models for additional transition mechanisms in the modelling framework. Considering for instance unintended interactions between specific system protection schemes could allow the analysis to reveal other critical events than those identified with the implementation demonstrated here. In this article, the framework was moreover combined with quasi-static contingency analysis, and the graph was used to structure results from (static) power flow simulations incorporated as part of the transition mechanism models. However, the general framework could also incorporate dynamic power flow simulations or be used to structure the results from existing simulation tools for cascading outages [6,13]. It could be used to structure historic outage and power interruption data if these include information about the transition mechanisms involved in the events.

iv) Accounting for uncertainties: Another key aspect of the methodology is that it explicitly acknowledges the uncertainty associated with critical sequences of events by assigning uncertainty estimates to their likelihoods. An advantage of the proposed uncertainty analysis methodology is that the it only requires the graph to be constructed once. We illustrated that although the resulting uncertainties may be very large, this information allows for prioritization of vulnerability-reducing measures. A possible direction for further work could thus be to investigate the effectiveness of different measures (e.g. grid reinforcement). Another direction could be to reduce the underlying uncertainties in barrier failure probabilities by incorporating more detailed simulation models for specific mechanisms (e.g. failure of islanding).

The present article focused on epistemic uncertainties associated with barrier failures, but in future work, the methodology could also be extended to account for additional aleatory as well as epistemic uncertainties. In particular, a promising extension would be to consider uncertainties associated with initiating events. One could for instance combine the modelling framework with models for the spatio-temporal variation of weather-related failure rates [26]. This could allow for capturing vulnerabilities to simultaneous failures and correlations due to the spatial location of transmission lines.

This article has demonstrated the methodology on a small but realistic test system to illustrate its advantages in a transparent manner. For further research it is proposed to investigate how the methodology scales for larger power system models. For large-scale applications of the modelling framework it may be necessary to implement fast search methods, e.g. based on [28,29], to guide the construction of the graph in a more intelligent manner. An interesting extension could be to combine the framework with optimization methods for identifying the most critical contingencies [35,36]: Considering critical consequences due to failure of islanding, one could first apply e.g. graph partitioning techniques [32] to identify contingency states with islands with large generation deficits, and then one could construct paths “backwards” towards possible initiating events. This suggestion for further work is in accordance with the underlying principle of the proposed modelling framework for vulnerability analysis, namely to focus on the sequences of events with potentially critical consequences.

CRediT authorship contribution statement

Iver Bakken Sperstad: Conceptualization, Investigation, Methodology, Project administration, Validation, Visualization, Writing - original draft. **Espen Hafstad Solvang:** Data curation, Investigation, Methodology, Software, Validation, Visualization, Writing - original draft. **Sigurd Hofsmo Jakobsen:** Conceptualization, Investigation, Methodology, Validation, Writing - review & editing.

Data resource

Data available in data repository Dryad at https://zenodo.org/record/3491916.

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

The research leading to these results has received funding through the project "Analysis of extraordinary events in power systems" (Grant No. 255226), co-funded by the Research Council of Norway, Statnett and Fingrid. The authors would like to thank the project partners and collaborators and in particular Gerd Kjølle, Oddbjørn Gjerde and Erlend Sandø Kiel for input and discussion of related work.

References

[1] Pourbeik P, Kundur PS, Taylor CW. The anatomy of a power grid blackout - root causes and dynamics of recent major blackouts. IEEE Power Energ Mag 2006;4(5):22–9. https://doi.org/10.1109/MPAE.2006.1687814.
[2] 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.
[3] Hillberg E. Perception, prediction and prevention of extraordinary events in the power system [PhD thesis]. Norwegian University of Science and Technology; 2016.
[4] Sperstad IB, Kjølle GH, Gjerde O. A comprehensive framework for vulnerability analysis of extraordinary events in power systems. Reliab Eng Syst Saf 2020;196:106788. https://doi.org/10.1016/j.ress.2019.106788.
[5] 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.
[6] 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.
[7] 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(6):4887–900. https://doi.org/10.1109/TPWRS.2016.2518660.
[8] Guo H, Zheng C, Iu HH-C, Fernando T. A critical review of cascading failure analysis and modeling of power system. Renew Sustain Energy Rev 2017;80:9–22. https://doi.org/10.1016/j.rser.2017.05.206.
[9] Kjølle GH, Gjerde O, Hofmann M. Vulnerability and security in a changing power system - executive summary report no. TR A7278 Trondheim, Norway: SINTEF Energy Research; 2013.
[10] Kjølle GH, Gjerde O. Vulnerability analysis related to extraordinary events in power systems. In: 2015 IEEE PowerTech; 2015. doi:10.1109/PTC.2015.7232388.
[11] Doorman GL, Uhlen K, Kjølle GH, Huse ES. Vulnerability analysis of the Nordic power system. IEEE Trans Power Syst 2006;21(1):402–10. https://doi.org/10.1109/TPWRS.2005.857849.
[12] Sperstad IB, Kiel ES. Development of a qualitative framework for analysing high-impact low-probability events in power systems. In: European Safety & Reliability Conference (ESREL) 2018; 2018.
[13] Henneaux P, Ciapessoni E, Cirio D, Cotilla-Sanchez E, Diao R, Dobson I, et al. Benchmarking quasi-steady state cascading outage analysis methodologies. 2018 IEEE international conference on probabilistic methods applied to power systems (PMAPS) IEEE; 2018. https://doi.org/10.1109/PMAPS.2018.8440212.
[14] Carreras BA, Newman DE, Dobson I, Poole AB. Initial evidence for self-organized criticality in electric power system blackouts. Proceedings of the 33rd annual Hawaii international conference on system sciences IEEE; 2000. https://doi.org/10.1109/HICSS.2000.926768.
[15] Carreras BA, Newman DE, Dobson I, Poole AB. Evidence for self-organized criticality in a time series of electric power system blackouts. IEEE Trans Circuits Syst I Regul Pap 2004;51(9):1733–40. https://doi.org/10.1109/TCSI.2004.834513.
[16] Dobson I, Carreras BA, Newman DE. A branching process approximation to cascading load-dependent system failure. In: 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the; 2004. doi:10.1109/HICSS.2004.1265185.
[17] Dobson I, Carreras BA, Newman DE. Branching process models for the exponentially increasing portions of cascading failure blackouts. Proceedings of the 38th annual Hawaii international conference on system sciences 2005. https://doi.org/10.1109/HICSS.2005.125.
[18] Dobson I, Zhou K, Carrington N, Wang Z, Carreras BA, Reynolds-Barredo JM. Exploring cascading outages and weather via processing historic data. In: Hawaii International Conference on System Sciences, Big Island, Hawaii; 2018.
[19] Nakarmi U, Naeini MR, Hossain MJ, Hasnat MA. Interaction graphs for reliability analysis of power grids: A survey; 2019. arXiv:1911.00475.
[20] Cuadra L, Salcedo-Sanz S, Del Ser J, Jiménez-Fernández S, Geem Z. A critical review of robustness in power grids using complex networks concepts. Energies 2015;8(9):9211–65. https://doi.org/10.3390/en8099211.
[21] Pagani GA, Aiello M. The power grid as a complex network: A survey. Physica A 2013;392:2688–700. https://doi.org/10.1016/j.physa.2013.01.023.
[22] Wang Z, Scaglione A, Thomas RJ. A Markov-transition model for cascading failures in power grids. In: 2012 45th Hawaii International Conference on System Sciences; 2012. p. 2115–24. doi:10.1109/HICSS.2012.63.
[23] Rahnamay-Naeini M, Wang Z, Mammoli A, Hayat MM. A probabilistic model for the dynamics of cascading failures and blackouts in power grids. 2012 IEEE power and energy society general meeting 2012. https://doi.org/10.1109/PESGM.2012.6345574.
[24] Rahnamay-Naeini M, Wang Z, Ghani N, Mammoli A, Hayat MM. Stochastic analysis of cascading-failure dynamics in power grids. IEEE Trans Power Syst 2014;29(4):1767–79. https://doi.org/10.1109/TPWRS.2013.2297276.
[25] Perkin S, Hamon C, Kristjánsson R, Stefánsson H, Jensson P. Framework for trajectory-based probabilistic security assessment of power systems. IET Gener Transmiss Distrib 2019;13(7):1088–94. https://doi.org/10.1049/iet-gtd.2018.5396.
[26] Kiel ES, Kjølle GH. The impact of protection system failures and weather exposure on power system reliability. 2019 IEEE international conference on environment and electrical engineering and 2019 ieee industrial and commercial power systems Europe (EEEIC/ I CPS Europe) 2019. https://doi.org/10.1109/EEEIC.2019.8783388.
[27] Carreras BA, Newman DE, Dobson I. Determining the vulnerabilities of the power transmission system. In: 2012 45th Hawaii International Conference on System Sciences; 2012. p. 2044–53. doi:10.1109/HICSS.2012.208.
[28] Yao R, Huang S, Sun K, Liu F, Zhang X, Mei S, et al. Risk assessment of multi-timescale cascading outages based on Markovian tree search. IEEE Trans Power Syst 2017;32(4):2887–900. https://doi.org/10.1109/TPWRS.2016.2618365.
[29] Ma Z, Liu F, Shen C, Wang Z, Mei S. Fast searching strategy for critical cascading paths toward blackouts. IEEE Access 2018;6:36874–86. https://doi.org/10.1109/ACCESS.2018.2846022.
[30] Hines PDH, Dobson I, Rezaei P. Cascading power outages propagate locally in an influence graph that is not the actual grid topology. IEEE Trans Power Syst 2017;32(2):958–67. https://doi.org/10.1109/TPWRS.2016.2578259.
[31] Zhou K, Dobson I, Wang Z, Roitershtein A, Ghosh AP. A Markovian influence graph formed from utility line outage data to mitigate large cascades. IEEE Trans Power Syst 2020;35(4):3224–35. https://doi.org/10.1109/TPWRS.2020.2970406.
[32] Lesieutre BC, Roy S, Donde V, Pinar A. Power system extreme event screening using graph partitioning. In: 2006 38th North American Power Symposium; 2006. p. 503–10. doi:10.1109/NAPS.2006.359618.
[33] Donde V, Lopez V, Lesieutre B, Pinar A, Yang C, Meza J. Identification of severe multiple contingencies in electric power networks. Proceedings of the 37th annual North American power symposium, 2005 2005. p. 59–66. https://doi.org/10.1109/NAPS.2005.1560502.
[34] Donde V, Lopez V, Lesieutre B, Pinar A, Yang C, Meza J. Severe multiple contingency screening in electric power systems. IEEE Trans Power Syst 2008;23(2):406–17. https://doi.org/10.1109/TPWRS.2008.919243.
[35] Pinar A, Meza J, Donde V, Lesieutre B. Optimization strategies for the vulnerability analysis of the electric power grid. SIAM J Optim 2010;20(4):1786–810. https://doi.org/10.1137/070708275.
[36] Cuffe P. A comparison of malicious interdiction strategies against electrical networks. IEEE J Emerg Sel Top Circ Syst 2017;7(2):205–17. https://doi.org/10.1109/JETCAS.2017.2704879.
[37] Phadke A, Thorp J. Expose hidden failures to prevent cascading outages [in power systems]. IEEE Comput Appl Power 1996;9(3):20–3. https://doi.org/10.1109/67.526849.
[38] Chen J, Thorp JS, Dobson I. Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model. Int J Electr Power Energy Syst 2005;27:318–26. https://doi.org/10.1016/j.ijepes.2004.12.003.
[39] Chen Q, McCalley JD. Identifying high risk N-k contingencies for online security assessment. IEEE Trans Power Syst 20(2). doi:10.1109/TPWRS.2005.846065.
[40] Kjølle GH, Gjerde O. The OPAL methodology for reliability analysis of power systems report no TR A7175 Trondheim, Norway: SINTEF Energy Research; 2012.
[41] Vadlamudi VV, Gjerde O, Kjølle G. Dependability and security-based failure considerations in protection system reliability studies. In: IEEE PES ISGT Europe 2013; 2013. https://doi.org/10.1109/ISGTEurope.2013.6695264.
[42] Dobson I, Flueck A, Aquiles-Perez S, Abhyankar S, Qi J. Towards incorporating protection and uncertainty into cascading failure simulation and analysis. 2018 IEEE international conference on probabilistic methods applied to power systems (PMAPS) 2018. https://doi.org/10.1109/PMAPS.2018.8440217.
[43] Gjerde O, Kjølle GH, Detlefsen NK, Brønmo G. Risk and vulnerability analysis of power systems including extraordinary events. In: 2011 IEEE PowerTech, Trondheim, Norway; 2011. doi:10.1109/PTC.2011.6019251.
[44] Vadlamudi VV, Hamon C, Gjerde O, Kjølle G, Perkin S. On improving data and models on corrective control failures for use in probabilistic reliability management. 2016 international conference on probabilistic methods applied to power systems (PMAPS). IEEE 2016. https://doi.org/10.1109/PMAPS.2016.7764089.
[45] Sperstad IB, Jakobsen SH, Gjerde O. Modelling of corrective actions in power system reliability analysis. In: PowerTech 2015; 2015. doi: 10.1109/PTC.2015.7232453.
[46] Karangelos E, Wehenkel L. Post-contingency corrective control failure: a risk to neglect or a risk to control? International conference on probabilistic methods applied to power systems (PMAPS) 2018. https://doi.org/10.1109/PMAPS.2018.

8440348.
[47] Karangelos E, Wehenkel L. An iterative AC-SCOPF approach managing the contingency and corrective control failure uncertainties with a probabilistic guarantee. IEEE Trans Power Syst 2019:3780–90. https://doi.org/10.1109/TPWRS.2019.2902486.
[48] Uhlen K, Kjølle GH, Løvås GG, Breidablikk O. A probabilistic security criterion for determination of power transfer limits in a deregulated environment. In: CIGRE Session, Paris; 2000.
[49] Trodden P, Bukhsh W, Grothey A, McKinnon K. MILP formulation for controlled islanding of power networks. Int J Electr Power Energy Syst 2013;45(1):501–8. https://doi.org/10.1016/j.ijepes.2012.09.018.
[50] Aven T, Zio E, Baraldi P, Flage R. Uncertainty in risk assessment: the representation and treatment of uncertainties by probabilistic and non-probabilistic methods. Wiley; 2014.
[51] 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. https://doi.org/10.1016/j.ijepes.2017.11.047.
[52] Chartrand G, Zhang P. A first course in graph theory. Dover Publications; 2012.
[53] UCTE. UCTE operation handbook. Union for the Coordination of the Transmission of Electricity (UCTE); 2004.
[54] International Electrotechnical Commission (IEC), International electrotechnical vocabulary (IEV): 192: Dependability/ primary failure.
[55] International Electrotechnical Commission (IEC), International electrotechnical vocabulary (IEV): 603: Generation, transmission and distribution of electricity - dependability and quality of service of electric power systems/ outage occurrences in electric power.
[56] 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(2):1528–36. https://doi.org/10.1109/TPWRS.2016.2588881.
[57] Gjerde O, Kjølle G, Jakobsen SH, Vadlamudi VV. Enhanced method for reliability of supply assessment - an integrated approach. In: 2016 Power Systems Computation Conference (PSCC), Genoa; 2016. https://doi.org/10.1109/PSCC.2016.7540989.
[58] Wehenkel L. Emergency control and its strategies. In: Proc. of the 13th Power Systems Computation Conference (PSCC), Trondheim, Norway; 1999.
[59] International Electrotechnical Commission (IEC), International electrotechnical vocabulary (IEV): 603: Generation, transmission and distribution of electricity - power systems planning and management/ island (in a power system).
[60] Milano F. Power system modelling and scripting. Springer Science & Business Media; 2010.
[61] Peixoto TP. The graph-tool python library 2014. https://doi.org/10.6084/m9.figshare.1164194.
[62] Zimmerman RD, Murillo-Sanchez CE, Thomas RJ. MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education. IEEE Trans Power Syst 2011;26:12–9. https://doi.org/10.1109/tpwrs.2010.2051168.
[63] Gjerde O, Aleixo L, Warland L, Døskeland IH. Integrated approach for reliability of electricity supply analysis - studies of demonstration network. In: Proceedings of the 2012 CIGRE Session, Paris; 2012.
[64] Sperstad IB, Solvang EH, Jakobsen SH. Four-area test network. doi:10.5281/zenodo.3491916.
[65] Kjølle G, Eggen AO, Vefsnmo HM, Heggset J, Bostad A, Trøtscher T, et al. Norwegian disturbance management system and database. In: Proceedings of the 2016 CIGRE Session, Paris; 2016.
[66] Kjølle GH, Sperstad IB, Jakobsen SH. Interruption costs and time dependencies in quality of supply regulation. In: 2014 International Conference on probabilistic methods applied to power systems (PMAPS), Durham; 2014. doi:10.1109/PMAPS.2014.6960620.