SINTEF

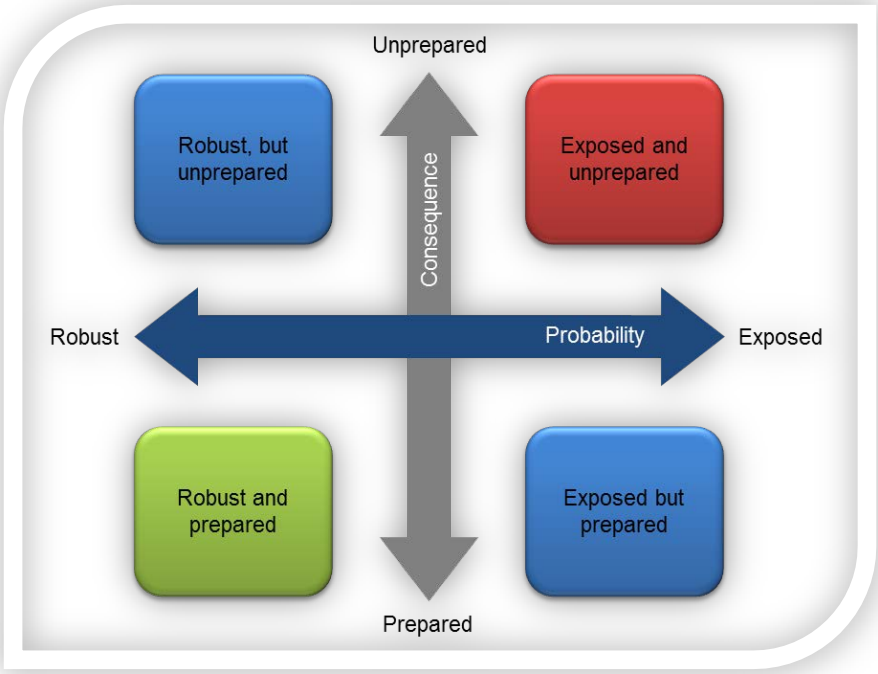
TR A7278- Unrestricted

Report

Vulnerability and security in a changing power system

Executive summary

Author(s)
Gerd H. Kjølle
Oddbjørn Gjerde
Matthias Hofmann



SINTEF Energy Research
Electric Power Systems
2013-07-25

SINTEF Energi AS
SINTEF Energy Research
Address:
Postboks 4761 Sluppen
NO-7465 Trondheim
NORWAY
Telephone:+47 73597200
Telefax:+47 73597250
energy.research@sintef.no
www.sintef.no/energi
Enterprise /VAT No:
NO 939 350 675 MVA

KEYWORDS:
Vulnerability
Security of supply
Extraordinary events
Power systems

Report

Vulnerability and security in a changing power system

Executive summary

VERSION
1.0

DATE
2013-07-25

AUTHOR(S)
Gerd H. Kjølle
Oddbjørn Gjerde
Matthias Hofmann

CLIENT(S)
Research Council of Norway, multiple clients

CLIENT'S REF.
Erland Staal Eggen

PROJECT NO.
12X618

NUMBER OF PAGES
51

ABSTRACT
This report presents the main results from the knowledge-building project Vulnerability and security in a changing power system. The main stakeholders of this project are the energy authorities, system operators and network companies. The project has emphasized vulnerabilities in relation to extraordinary events with low probability to occur and high impact on the security of electricity supply, like wide-area power supply interruptions. It is of great importance to study how vulnerability in power systems evolves and if the probability of wide-area interruptions is increasing, due to ageing, increased utilization and operational stress, increasing dependencies on ICT, new operating scenarios, etc. For this purpose, we need methods to analyse and identify vulnerability as well as indicators that can be used to measure and monitor vulnerability. The main contributions from this project are:

- A framework for monitoring and classifying vulnerabilities in electric power grids.
- A methodology for risk and vulnerability analysis emphasizing extraordinary events.
- Recommendation of risk analysis methods aiming to increase the power system's operational security.
- Case studies illustrating the development of vulnerability indicators and methods and the use.

PREPARED BY
Gerd H. Kjølle

SIGNATURE
GKj

CHECKED BY
Maria D. Catrinu-Renström

SIGNATURE
dlC

APPROVED BY
Knut Samdal

SIGNATURE

REPORT NO.	ISBN	CLASSIFICATION	CLASSIFICATION THIS PAGE
TR A7278	978-82-594-3540-8	Unrestricted	Unrestricted

SINTEF

Table of contents

1 Introduction

This report represents the executive summary of the results from the knowledge-building project Vulnerability and security in a changing power system, conducted in the period 2009 – 2012 (2013). The main stakeholders of this project are the energy authorities, system operators and network companies. The project has been funded by the Research Council of Norway and the following (mainly Norwegian) partners:

- Norwegian Water Resources and Energy Directorate (NVE)
- Norwegian Directorate for Civil Protection and Emergency Planning (DSB)
- Energy Norway (Energi Norge)
- Statnett
- Hafslund Nett
- NTE Nett
- Troms Kraft Nett
- Fortum Distribution
- Skagerak Nett
- BKK Nett
- Lyse Elnett
- Eidsiva Nett.

The aim of this project has been to build competence and knowledge regarding vulnerabilities in the electric power system in a changing environment, such as, integration of distributed generation and smarter energy networks, as well changing operating conditions. The objectives were to:

- Establish a scientific basis for monitoring and management of vulnerabilities in the power system.
- Provide a methodical framework for vulnerability analyses in the development and operation of the transmission and distribution systems.

The project has emphasized extraordinary events, i.e., failures and disturbances in the power grids leading to wide-area interruptions or long-lasting interruptions with severe impact on society. The significant contributions from this project are:

- A framework of definitions, indicators and methods that can be used to monitor and classify vulnerabilities in electric power grids.
- Methods and tools for enhanced power system risk and vulnerability analysis, with particular emphasis on extraordinary events.
- Risk analysis methods for extraordinary events, aiming to increase the operational security and/or utilization of the power system.
- Case studies to illustrate the development and use of vulnerability indicators and methods.

Increased knowledge about the vulnerabilities in power systems is of utmost importance to ensure the security of electricity supply. It enables the development of a secure and flexible power system both on a regional and national level, and contributes to further development of the regulatory framework. Through in-depth power system risk and vulnerability studies, the project has not only contributed to the knowledge-building within the electric power sector but also provided input to the societal security area regarding critical infrastructures.

This report is organised as in the following. Chapter 2 gives the background and motivation for the project and the vulnerability framework is outlined in Chapter 3. The main results from the project are described in Chapter 4. Conclusions and recommendations are given in Chapter 5. The main terms and definitions used are presented in Appendix A.1.

2 Security of electricity supply in a changing power system

Society is critically dependent on electricity to maintain its functionality and cover basic needs such as food and water supply, heating, safety, financial services, etc. As a consequence, a secure electricity supply is critical for the society. Thus, the electric power system is one of society's critical infrastructures defined as physical and logical systems essential for social welfare [1-3]. Other examples are transport networks, electronic communications and water and sewage systems.

Strained power situations in the Nordic power market resulting in very high electricity prices during winter 2009/2010 and 2010/2011 and the storm Dagmar in the Nordic countries in December 2011, causing devastating damages of lines and wide-area interruptions, are all examples of events in later years which have brought increased attention to the security of electricity supply. Such events receive a lot of media attention, bringing about speculations if the vulnerability of the power system is increasing due to lack of maintenance, workforce reductions, ageing components, increased utilization of the power system, etc. This was the situation before this project started, making it topical to increase the knowledge on vulnerabilities in particular. It is an aim that the results of the project contribute to the knowledge base needed to ensure an appropriate level of security of supply.

2.1 Security of electricity supply

Security of electricity supply means the ability of an electricity system to supply final customers with electricity [4]. It is composed of energy availability, power capacity and reliability of supply, with long term (system adequacy) and short term (operational security) perspectives [5]. Energy availability and power capacity are measured by the energy and power balance. Reliability is measured by power system failures and the consequences in terms of number and duration of interruptions [6]. What matters also, is the severity of interruptions which can be measured using indices like interrupted power (or disconnected load), energy not supplied and the corresponding societal cost (e.g. CENS [7]).

The main unwanted events which can threaten the security of electricity supply are energy shortage, capacity shortage or power system failures [8], or combinations of these. The consequences of shortages for society and end-users can be extremely high prices or curtailment, while failures can cause wide-area power supply interruptions (blackouts) and major harm to society [8, 9]. This project has focused on the latter types of events. Energy availability and power capacity are not studied in detail, but are taken into account as far as they affect the reliability. Energy and capacity shortage, or situations where components are out for maintenance or other causes, may give rise to strained power situations increasing the probability of wide-area interruptions.

According to the Norwegian energy regulator, security of electricity supply can be regarded as a generic term describing the overall robustness of the power system, where the term robustness covers energy security, power capacity security and the power system's ability to withstand extraordinary events [10]. Security of electricity supply is also discussed in the Norwegian TSO Statnett's system operation and market development plan [11]. In this project, an extraordinary event is defined as an event where power system failures lead to wide-area interruptions and blackouts. It is an event with high societal impact and low probability of occurrence, often denoted as a HILP event.

2.2 Extraordinary events

Power system failures occur occasionally in both the transmission and the distribution systems, most often with minor consequences. The power system at the transmission level is usually dimensioned and operated according to the N-1 criterion, meaning that the system should withstand loss of a single principal component without causing interruptions of electricity supply [12]. Distribution systems are mostly operated as radials and any component outage due to a failure will in general, lead to an interruption. The duration may be rather limited depending on reserve supply possibilities, e.g. by closing open ring main units.

Severe consequences of interruptions will most likely be caused by combinations of events. Examples are two or more failures in the main grid, malfunctioning of the protection system together with a failure in the main grid, grid failure overlapping outage of a large power plant, or storm causing damage on power lines. In distribution systems failures with severe consequences may, for example, be those resulting in loss of service in interconnected infrastructures such as transport and telecommunication.

Analyses of recent blackouts, e.g., [13-16], show that their causes often are on the system or organizational level, representing a combination of factors, for example:

- Strong winds and tree-fall (common causes) resulting in extensive damages of power lines [17].
- Malfunction of critical equipment such as protection and cable joints or sleeves [18, 19].
- Strained operating situations where the system is operated close to its limits [16, 20]
- Human factors – lack of situational awareness and lack of coordination and planning of activities that may have an impact on the power system (for example digging work, etc.) [13, 19].

Extraordinary events, involving coinciding failures and severe consequences, are usually regarded to have low probability (HILP events). Many blackouts that have occurred during the last decades are thoroughly described in the literature, e.g. [8, 21-24]. Examples are shown in Figure 2-1where the blackouts are classified according to the amount of disconnected load and stipulated average (weighted) duration. The largest in terms of disconnected load was the US/Canada blackout in 2003, while the largest in terms of interruption duration was the Canadian ice-storm in 1998, followed by the Steigen event in Norway in 2007 and the storm Gudrun in Sweden in 2005.

Most of the events in Figure 2-1 have occurred in the transmission system. The storm Gudrun, the Steigen event and the event at Oslo central station (Oslo S) are examples mainly affecting the distribution system and partly the sub-transmission. While the storm Gudrun affected a large area in Southern Sweden, the other two events had a more local character. Steigen, a small community with less than 3000 inhabitants in Northern Norway, lost its power supply for six days due to breakdown of both 66 kV lines supplying the community, caused by heavy storm. The event at Oslo S started as a minor fire in an 11 kV cable caused by digging work around the station. The fire led to evacuation and the station and its services was closed for 20 hours. Several communication systems were affected, including train operation services, internet and phone services for thousands of people. These events in the distribution system might not be regarded as wide-area interruptions, but can be classified as extraordinary as they caused long-lasting interruptions and had severe impact for a whole community and for critical societal functions.

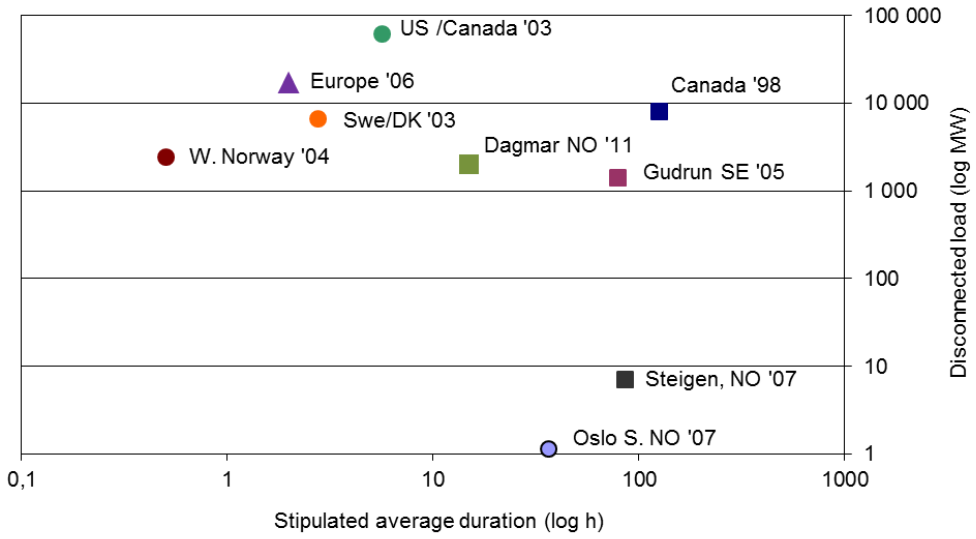


Figure 2-1 Stipulated duration and disconnected load for some historical blackouts.

2.3 Drivers for a changing power system

Through the fulfilment of climate agreements and strategies like the Norwegian Energi21, European EU202020 and the European electricity grid initiative (EEGI) [25-27], the power system is expected to undergo major changes in coming years due to massive integration of large scale renewables and distributed generation, changing power flows, transition to smarter grids, etc. Society's dependency on electricity will increase as a consequence of more use of ICT and new uses like smart meters, electrical vehicles and distributed electricity storage.

The current transmission and distribution system is built for the traditional power flow from large sources to demand. Low levels of capacity investments over many years have led to increasing utilization of the system and in many areas more strained operation and lowered security of electricity supply [28]. The system is generally an ageing infrastructure and the need for reinvestments is rapidly increasing. At the same time the climatic changes may impose increased stress on the grids.

Ageing components and systems and climate changes are challenges that critical infrastructures have in common. In addition there are challenges related to restructuring of organizations and outsourcing, terrorism, and globalisation (see, e.g., [2, 29]). Most critical infrastructures are also interdependent, because disruptions in one infrastructure may impact the functionality of other infrastructures, for example between electronic communications and the electric power system which depends on ICT systems for monitoring, protection and control. The complexity increases and coupling is getting tighter in critical infrastructures, in particular due to the inherent ICT control systems [2, 30, 31]. In the future power system (smart grids), the interdependencies and the complexity will increase due to new technologies, components and new ways of operating the power system.

To meet the challenges in the current power system and develop strategies for the future system, development plans and huge amounts of investments are allocated at European level, as described in the European Energy Infrastructure package (e.g. defining goals for European electricity highways) and

ENTSO-E's Ten Year Network Development plan, see e.g., [26, 32, 33]. On a national level, in Norway, the transmission system operator Statnett plans for investments in the order of NOK 50 - 70 billion up to 2020 [28]. The total grid investment plans for all grid levels in Norway add up to 130 billion NOK for the coming 10 year period, including investments in smart meters and interconnections to other countries [34]. In addition, there are plans for new power plant investments in the order of 40 - 50 billion NOK.

According to EEGI, a stronger and smarter grid is a precondition for ensuring security of electricity supply, a high quality of service and market access for all customers [27].While the reliability and robustness of the power system in general is expected to increase with new investments and smarter grids, the risk of extraordinary events might increase due to vulnerabilities caused by dependencies, increasing complexity, new components and technologies, cyber threats, new operating scenarios, etc.

In this environment it is of great importance to study how vulnerability and risk related to extraordinary events and wide-area interruptions evolves. The need for new and enhanced reliability standards is acknowledged in Europe as well as in North-America [26, 35, 36], comprising amongst other new types of indicators for monitoring and control of security of supply, and new tools and analysis techniques.

2.4 State of the art regarding monitoring of security of supply (in Norway)

The energy regulators and transmission system operators look at different factors to monitor long and short term development of security of supply. For example, the energy availability and capacity can be monitored following the energy and power balance, including import and export between countries in the interconnected Nordic power system and the development in electricity demand. For the energy availability in a hydro-dominated system like the Norwegian power system, it is important to monitor the hydro inflow and reservoir levels. Dry years with very low inflow are of particular interest for potential extraordinary situations. The power system (at the transmission level) is designed and operated according to the N-1 criterion. Thus, transmission capacities are monitored (at least for critical corridors), as well as congestions between areas and the degree of fulfilment of the N-1 criterion (see e.g., [37]).

Regulations relating to the transmission and distribution grids are continuously introduced and developed since the Energy Act was put into force in Norway in 1991, see e.g., [38]. Examples of regulations concerning the security of supply are the mandatory reporting of various technical and economic parameters such as investments, maintenance and reinvestments, failures and interruptions as well as costs of energy not supplied (CENS). The transmission system operator and network companies are also obliged to perform power system studies of the anticipated measures and investments, including risk and vulnerability analyses focusing on extraordinary events in the power system.

The Norwegian energy authorities and network companies follow the development in security of supply using information from the mentioned mandatory reporting and analyses, including the age development of the main components. Long term evaluation of the security of supply consists, amongst other, as a basis for granting concession for new generation, lines and transformers [39]. In addition, the short term frequency and voltage quality is monitored (see e.g., [40]). An important instrument for the energy authorities' monitoring of security of supply is the regular supervision of the companies and their compliance with the regulations. This supervision is conducted in co-operation by the energy regulator (NVE) and electricity authority (DSB).

The state of the art regarding security of supply and the use of indicators in other European countries are described in a small study conducted within the project [26].

2.5 The need for indicators and methods to monitor vulnerability

It is of great importance to study how vulnerability in power systems evolves and if the probability of wide-area interruptions is increasing, due to ageing, increased stress, new operating scenarios, etc. For this purpose, we need methods to analyse and identify vulnerability as well as relevant indicators that can be used to measure vulnerability. Previous studies have revealed the need for new knowledge and tools for monitoring vulnerability, e.g. [41, 42]. There are few, if any, indicators or data on an aggregate level to monitor and describe the vulnerabilities in quantitative terms and, for instance, to identify underlying mechanisms impacting the vulnerabilities.

Existing indicators in use are mostly performance indicators (describing security of supply). The best available data base for documenting the security of supply in terms of reliability is the fault statistics, which includes data on fault frequency, energy not supplied and the cost of energy not supplied [43, 44]. However, this data only contain information about the system components that have failed. Moreover, the performance indicators mainly deal with normal or frequent events, describing the historical development. New types of indicators are needed being capable of describing the risk exposure of the system and not only its performance.

In risk and vulnerability analysis of electric power systems a major challenge is to identify chains of events that could lead to wide-area interruptions. It is necessary to have knowledge about the underlying causes, as well as data and models for the determination of the probabilities for different initiating events, for the propagation of outages and for the determination and evaluation of the consequences of cascading outages. Beyond the traditional and deterministic N-1 criterion, there is no established framework on how to analyse and predict the security of electricity supply and vulnerabilities in electric power grids. A vulnerability analysis of the Nordic power system [41] revealed a lack of knowledge on what is a sufficient or acceptable level of security of electricity supply, and how to analyse extraordinary incidents with low probability and severe impact on society.

This situation calls for increasing the knowledge on monitoring and management of vulnerabilities and a methodical framework for handling vulnerability and security of supply in the development and operation of the transmission and distribution systems.

The project has addressed this knowledge gap through the development of frameworks and methods for monitoring vulnerability.

3 Vulnerability in power systems

This chapter describes the vulnerability framework developed in the project and the relationship between vulnerability, risk and extraordinary events. A few scenarios are outlined for the identification of threats and vulnerabilities in the current and future power system. Finally, the project and the project results are discussed in the context of risk and vulnerability management.

3.1 Vulnerability framework and definitions

Various definitions of vulnerability are found in the literature and there is apparently no widely accepted definition [43]. In general, vulnerability describes how a system faces problems to carry out its intended function when exposed to materialised threats. The following definition is adopted in the project (based on e.g., [9, 45]):

Vulnerability is an expression for the 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. Vulnerability is an internal characteristic of the system.

A system is vulnerable if it fails to carry out its intended function, its capacity is significantly reduced, or the system has problems recovering to normal function. This definition of vulnerability describes the dualistic concept of susceptibility towards threats and the coping capacity to recover from the unwanted event [45]. Figure 3-1 shows the internal and external dimensions of vulnerability. These are described in more detail further down.

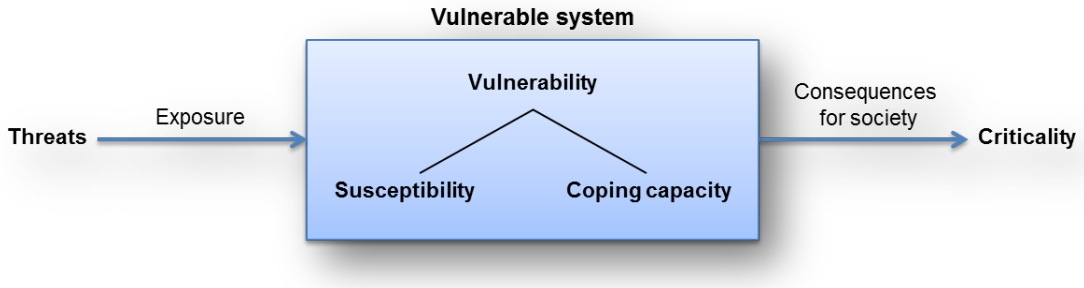


Figure 3-1 Internal and external dimensions of vulnerability [43].

Threat can be defined as any indication, circumstance, or event with the potential to disrupt or destroy a critical infrastructure, or any element thereof [1]. Threats are evolving outside of the vulnerable system and can be related to nature, humans or the operational conditions. Exposure is related to threats and describes how the system is exposed to different threats. A threat may lead to the unwanted event(s), here defined as power system failure(s) leading to interruption of electricity supply.

The various dimensions of vulnerability as presented in Figure 3-1 can be made more specific and categorized for the electric power system as elaborated in [43, 46] and illustrated in Figure 3-2. The three main categories of threats are shown to the left in the figure, i.e., natural hazards (e.g., major storm), operational (e.g., strained operation), and human unintended (e.g., errors, digging) and intended acts (e.g., terror, sabotage), respectively. In this framework all kinds of hazards or threats can be taken into account, representing an all-hazard approach [1, 2] to risk and vulnerability management.

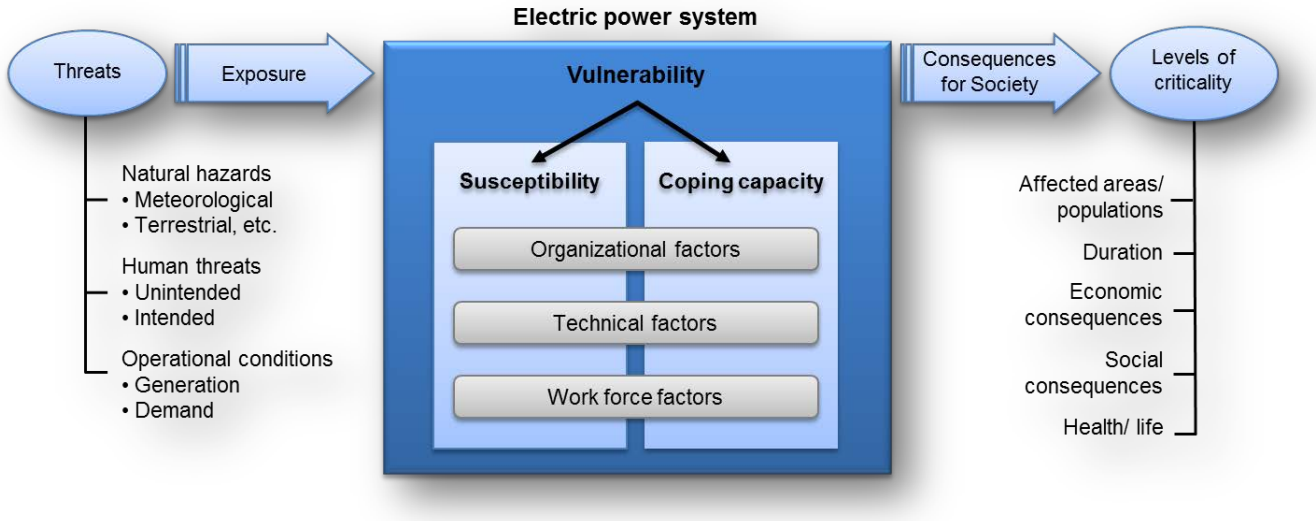


Figure 3-2 Theoretical framework for electric power system vulnerability, based on [43, 46].

The power system is susceptible to a threat if it leads to a disruption in the system. Susceptibility depends, e.g., on the technology, the work force and the organization. The coping capacity describes how the operator and the system itself can cope with the situation, limit negative effects, and restore the function of the system after a disruption (unwanted event). There are numerous factors that have an influence on the vulnerability (both susceptibility and coping capacity) [43]. These can be sorted in the three categories technical, work force and organizational as shown in Figure 3-2 and exemplified in Table 3-1.

Table 3-1 Examples of internal system factors with influence on susceptibility and coping capacity [46].

Influencing factors	Susceptibility	Coping capacity
Technical	Technical condition of components Operational stress Redundancies, N-1 criterion[1]	Equipment for repair Spare parts Redundancies, N-1 criterion
Human related (work force)	Availability of skilled personnel Operative competence Human errors	Availability of personnel Competence, skills in system restoration and repair of critical components
Organizational	Availability of information Coordination between operators Structure of the sector	Availability of communication Coordination of restoration Contingency plans

While Table 3-1 gives examples of internal vulnerability influencing factors, there are external factors on the system level that may influence the vulnerability. These comprise institutional factors related to the electricity market conditions, regulations of the grid operators, conditions for granting concessions of building new power lines, etc. Social factors such as, acceptance of building power lines and recruitment to the power sector, may also be important.

[1] N-1 criterion expresses the ability of the system to withstand loss of a single principal component without causing interruptions of electricity supply.

The term criticality in Figure 3-1 and Figure 3-2 refers to the level of criticality of consequences for the users of the infrastructure and not for the components in the system. The criticality can best be measured by the society's dependence on electricity supply. The extent of the consequences of an unwanted event (power system failure), is for instance directly dependent on factors like the affected population/area, duration of the interruption, type of customers, economic consequences, social consequences, and consequences for health and life. More examples of threats and factors influencing vulnerability and criticality are given in [43].

The framework presented in Figure 3-1 and Figure 3-2 represents the theoretical vulnerability framework for electric power systems in general. In this project, the electric power grid has been in focus in the development of vulnerability indicators. Hence, the vulnerable system is defined as the electric power grid. Included in the vulnerability influencing factors for susceptibility and coping capacity are the internal factors, i.e., those that the grid operators can control themselves. These factors should be defined within the system boundaries as seen from the grid operators. Generation and demand constitute operational conditions for the grid and hence, may be regarded as threats imposing operational stress on the grid. As such they are external factors, but since both to some extent can be controlled in the operation of the system, they are partly inside the system boundaries. Outside the boundaries there are also institutional and social factors as mentioned above. Institutional factors like regulations of the grid operators will, on the other hand, be inside the system boundaries as seen by the perspective of the energy authorities.

3.2 Risk of extraordinary events

While vulnerability is an internal characteristic of the system, risk can be defined as a combination of the probability and consequence of an unwanted event [47]. Vulnerability may affect both the probability and the consequence and is as such a component of risk. In Figure 3-1 and Figure 3-2 the combination of threats and susceptibility forms the probability of an unwanted event, while the combination of coping capacity and criticality gives the consequences. In addition to the factors shown in Table 3-1 the coping capacity might be hampered by additional threats, for instance traffic jam, bad weather or lack of daylight, thus, worsening the consequences.

The project Vulnerability and security in a changing power system has focused on vulnerabilities regarding extraordinary events with low probability and high impact on the security of electricity supply, like wide-area interruptions or blackouts. Such events are often denoted HILP (high impact, low probability) events. Hence, the risk of wide-area interruptions is a combination of the vulnerability to external threats that may lead to HILP events (depending on the coping capacity), and the potentially large societal consequences of power supply interruptions.

As can be seen by the categorisation of vulnerability influencing factors in Figure 3-2 and Table 3-1, many of these are human related, e.g., related to competence and skills, availability and organizational factors. Systems where people have important roles like the electric power system in general or the grid in particular are often referred to as socio-technical systems [48]. A socio-technical system contains several types of elements: physical (e.g., equipment, buildings), non-material (e.g., software, working procedures and practices), personnel, management (including policies, strategies, training, etc.) and the internal and external environment in which the system operates [48]. It is important in a risk analysis to consider all these elements and the interaction and interfaces between them. The system under study will also have interfaces with other systems that might come into consideration. For example, the interface between distribution and transmission system operators as well as the interaction with authorities, contractors and other parties might be important to take into account in a risk analysis related to extraordinary events. In addition, there are challenges in analysing the relationship between the above-mentioned elements due to the large complexity and tight coupling (interconnectedness) in socio-technical systems such as the electric power system.

3.3 Vulnerability in a changing power system

As outlined in Chapter 2, the power system is under change for a number of reasons. The electricity infrastructure and business sector are exposed to continuously changing external conditions, due to climate change, increasing electricity consumption, new operating scenarios, increasing dependencies on ICT, changes in the regulation of grid operators, etc. In an early phase of this project, a few scenarios were described focussing on vulnerabilities in the future power system originating from drivers and challenges raised above and in Chapter 2. The objective was to describe scenarios for a changing power system, enabling the identification of threats, vulnerabilities and risks and the need for analytical tools. This activity has also provided input to the vulnerability framework presented in this chapter.

The scenarios were described along the risk dimensions for unwanted events, i.e., one dimension for the probability and another for the consequences. Here, the consequences are related to the power system itself and the coping capacity characterised by 'prepared' versus 'unprepared'. The probability of unwanted events is characterised by 'robust' versus 'exposed'. The two dimensions are shown in Figure 3-3.

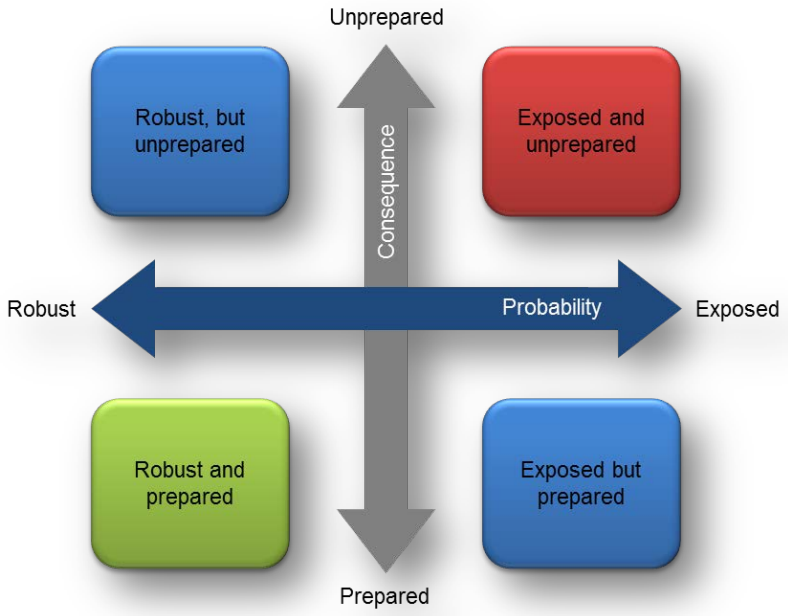


Figure 3-3 Risk dimensions for vulnerability in the current and future power system.

The main drivers for vulnerabilities in a changing power system described in Chapter 2 can be summarized as three main challenges:

- Increasing strains (weather-related and/or operational)
- Limited access to personnel and critical competence
- Increasing dependencies, complexity and uncertainties.

An important question is how these challenges will affect vulnerability (susceptibility and coping capacity) and the risk of extraordinary events, i.e., probability of power system failures (unwanted events) and the ability to handle power system failures and limit the consequences.

Table 3-2 outlines several scenarios for the Norwegian power system in 2030. Many scenario studies regarding power systems which are reported in literature are directed towards 2020 or 2050. In this project, 2030 was chosen as it represents a stage sufficiently far ahead, while the current assets still play a major role in the power system.

Table 3-2 Scenarios for the future Norwegian power system of 2030.

Scenario	Main drivers and characteristics
Status quo	**Business as usual, casual adaptation** to regulations and new loads, necessary maintenance. However, limited new investments, outsourcing of skilled people, etc.
Ageing and Outdated	**Ageing of assets and competence**. Lack of new grid investments, limited maintenance. Increased electricity consumption and generation. Difficult to recruit skilled people.
Techno Grid	**Massive integration of distributed generation, active grids and users**, electrification of transport, more automation and ICT. Attractive business sector for new skilled recruits.
Gone with the Wind	**Climate change and extreme weather**. More extreme winds, high ice loads, etc. Stronger design criteria, new grid investments and increased emergency preparedness.

The scenarios in Table 3-2 go in different directions regarding vulnerabilities along the two dimensions probability and consequence. Examples of vulnerabilities in each of the scenarios are:

- Status quo
  - Vulnerable to strained operating situations, dependent on contractors
- Ageing and Outdated
  - Poor technical condition of assets in some parts of the grid, lack of skilled personnel
- Techno Grid
  - Tighter coupling to and interdependencies with other infrastructures (ICT), increased complexity, however, more robust due to new investments
- Gone with the Wind
  - Exposed to weather, restoration delayed by bad weather.

All these scenarios for the development of the Norwegian system should, in addition, include a broader perspective: the increasing integration with Europe in terms of interconnections and power exchange as well as the influence of European objectives and strategies for development of the electric power system up to 2020 and 2050. Factors like changing power flows due to increased renewable generation, price differences, balancing power, etc., will likely influence the assessment of vulnerability in all scenarios. It is uncertain, however, how the integration with Europe will affect the Norwegian situation.

The scenarios described in Table 3-2 are based on a foresight-process. They are not complete scenario descriptions and are not meant to fill the whole risk and vulnerability picture. These scenarios together with analyses of historical blackouts and cases (see Chapter 4), have served as a basis for the development of the vulnerability framework, indicators and analysis methods.

3.4 Risk and vulnerability management

The relationship between risk, vulnerability and extraordinary events is described in the previous section. Risk management on the company level is composed of risk assessment and risk control, where assessment consists of analysis and evaluation [48]. Risk management is in general defined as a continuous management process with the objective to identify, analyse, and assess potential hazards in a system or related to an activity, and to identify and introduce risk control measures to eliminate or reduce potential harms to people,

the environment, or other assets [48]. According to [48], risk management is a continuous management process, which often contains six elements as described below and illustrated in Figure 3-4. Since this project has especially dealt with vulnerabilities, the elements of risk management are here adapted to vulnerability management in the context of extraordinary events (wide-area interruptions or blackouts), i.e., events threatening the security of electricity supply:

- Identify
  - Identify threats and potential unwanted events (here: power system failures with the potential of causing wide-area interruptions)
- Analyse
  - Identify critical assets, locations etc., and the severity of harm if the unwanted event happens
- Plan
  - Develop actions to address individual threats, prioritise vulnerability reducing actions, etc.
- Track
  - Monitor the (risk and) vulnerability level and actions to reduce the vulnerability
- Control
  - Execute and control proposed vulnerability reducing actions
- Communicate and document
  - Risk communication. A system for documentation and tracking of risk and vulnerability decisions must be implemented.

Figure 3-4 Continuous risk and vulnerability management process, based on [48].

This project has dealt with the three elements 'identify', 'analyse' and 'track', where the objectives have been to provide framework and methods for risk and vulnerability analysis and vulnerability indicators. In addition, case studies and analyses of historical extraordinary events were performed. The main results are presented in Chapter 4.

Power supply interruptions lead to direct consequences for the end-users and will in general have an impact on other dependent infrastructures and their services. Extraordinary events such as wide-area interruptions and blackouts have a severe impact on critical societal functions and need to be addressed from a societal security point of view. Societal security can be defined as the ability of the society to maintain critical societal functions and safeguard the citizens' life, health and basic needs during big stresses or large unwanted events due to various types of intended acts, accidents or natural hazards [49].

In this perspective, it is important not only to identify and understand the causes of an extraordinary event and prevent it from happening, but also to deal with the consequences in a best way, i.e., to prepare for, respond to and recover from the event. This involves interaction between technological, human, organizational and societal factors as shown in Figure 3-2. The different phases of dealing with societal security and vulnerability management related to extraordinary events can be illustrated as in Figure 3-5, based on various sources (e.g., [48-50]). The main activities in each phase are indicated:

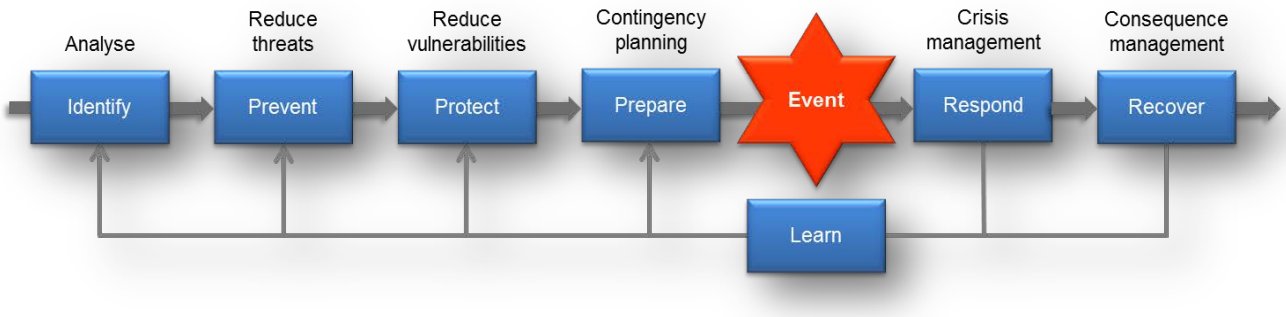


Figure 3-5 Phases of vulnerability management related to extraordinary events.

While the process shown in Figure 3-4 describes the different phases and elements in a continuous risk and vulnerability management on a company level, Figure 3-5 describes the phases of vulnerability management related to the extraordinary event. As illustrated in the figure, it is important to incorporate feedback in the various phases from lessons learned after the event. Training and exercises are also important parts of dealing with extraordinary events [51, 52].

Relating to Figure 3-5, the results of this project support mainly the first four phases 'identify', 'prevent', 'protect' and 'prepare' as well as the learning phase. Thus, the results provide a decision basis for a better contingency planning and crisis management.

4 Main results of the project Vulnerability and security in a changing power system

4.1 Overview of main results

The project work in Vulnerability and security in a changing power system has been organized in five different work packages as shown in Figure 4-1. A range of different types of activities have taken place, as indicated in the figure, consisting of literature surveys, analyses of historic extraordinary events and fault and interruption statistics, working with scenarios/foresight processes, case studies, development of frameworks and vulnerability indicators, methods and examples of indicators.

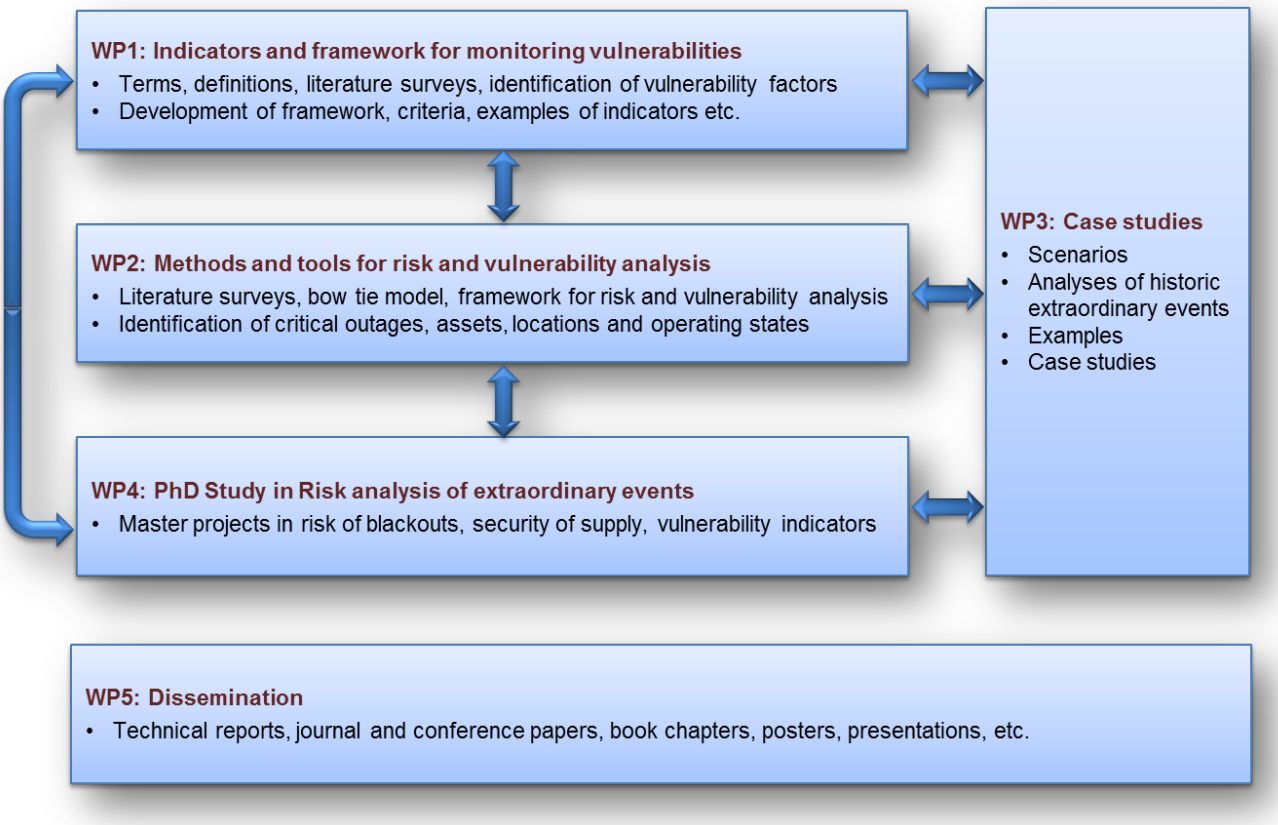


Figure 4-1 Work packages and activities in Vulnerability and security in a changing power system.

This chapter gives a description of the main results from the work packages WP1 – WP3 regarding methods for analysis and identification of vulnerability, vulnerability indicator development and case studies. The results regarding literature review and state of the art as part of WP1, are elaborated in [43], while the definitions and vulnerability framework is outlined in Chapter 3. The papers and presentations from the PhD study in WP4 are included in the total list of publications from the project as listed in this chapter. Collaboration with national and international partners, workshops and seminars are briefly described. These have been important arenas for discussions and inputs to the project work.

The work and partial results achieved on the way in this project provided basis for input to consultation responses and new research ideas. On the national level, the project provided recommendations regarding regulations of network companies and input to Norwegian official reports with respect to security of

electricity supply. Furthermore, the results have served as basis for new ideas for research on a national level providing input to two project applications for 2013 in the ENERGIX programme at Research Council of Norway (RCN). Moreover, the project work has provided input to the plan for the new research programme in Societal Security at RCN regarding critical infrastructures.

On the international level, the project provided input to work programs and call texts in the area of smart energy networks in the seventh European Framework Programme of research (EU 7FP). In addition, the project results have served as input to the EU 7FP project AFTER (2011 – 2014) on risk and vulnerability assessment in the combined power and ICT system and to the European Energy Research Alliance (EERA) joint programme on smart grids, sub-programme transmission networks [53]. The vulnerability framework developed in the project is adopted in the description of work for the GARPUR EU 7FP-project (2013) within advanced concepts for reliability assessment of the pan-European power system [54].

4.2 Analysis and identification of vulnerability

4.2.1 The bow tie model

The framework for vulnerability analysis is based on the conceptual bow tie-model describing the relations between main causes and consequences of an unwanted event [24, 48, 55]. Figure 4-2 gives an example where the main unwanted events to be considered are power system failures potentially leading to wide-area interruptions or blackouts, i.e., severe (major, critical or catastrophic) consequences. The figure shows the main categories of threats (or causes), which include natural hazard, technical/operational, human errors and intended acts such as terror or sabotage.

The threats might lead to power system failures through a set of causes, while failures might lead to different consequences through a set of circumstances.

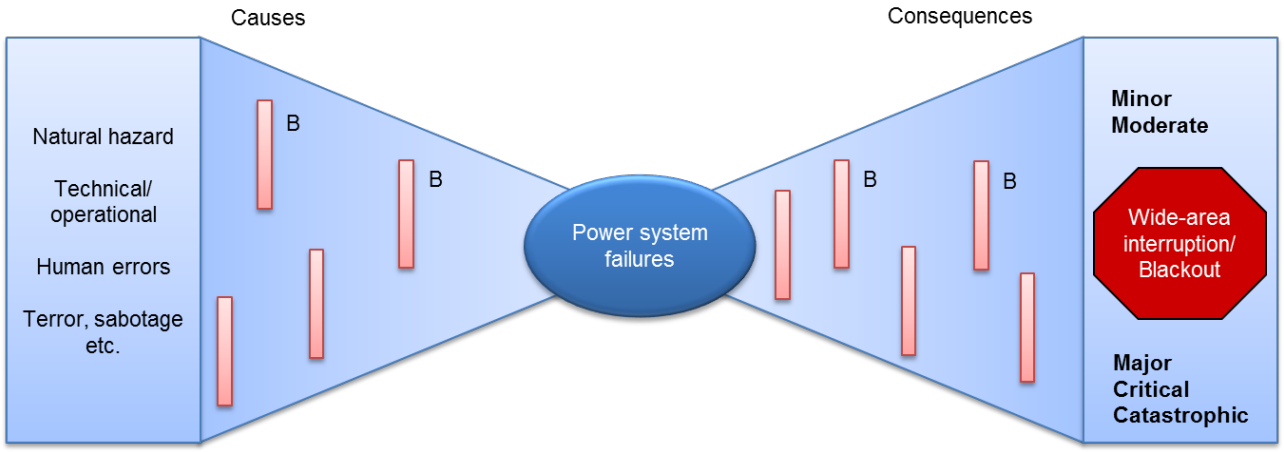


Figure 4-2 Threats, unwanted event[2] (power system failures), consequences and barriers (B).

[2] Here, we use the term 'unwanted event' synonymously with 'undesired event' used e.g., in 31. Hokstad, P., I.B. Utne, and J. Vatn, eds. *Risk and interdependencies in Critical Intrastructures*. Springer series in Reliability Engineering. 2012, Springer: London.

The bow tie model is a concept for helping to structure and visualize the causes and consequences of unwanted (extraordinary) events as a basis for the risk and vulnerability analysis. To the left in the bow tie model, possible causes behind the unwanted event are listed. The potential consequences are shown to the right. The starting point for the analysis is the unwanted event (power system failures). An important part of the causal analysis is to establish the relationship between the unwanted event and the basic causes. This is often performed using fault tree analyses, while the consequences might be analysed by using event tree analyses [48]. In this project, a bow tie model in Matlab Simulink is developed using fault and event trees.

As indicated in the figure, a number of barriers (B) exist to prevent threats from developing into unwanted events and to prevent or reduce the consequences of unwanted events. A system is more vulnerable towards the relevant threats if the barriers are weak or malfunctioning. There are different component or system oriented barriers to prevent failures, and different barriers related to restoration of supply and the end-users' consequences. The barriers can be grouped in two parts; one on the causal side related to the threats and susceptibility. The other is on the consequence side related to the coping capacity and consequences. Examples are given in Table 4-1. Comparing these examples with the vulnerabilities (susceptibility and coping capacity) exemplified in Table 3-1 it can be noticed that the vulnerabilities are closely related to the barriers.

Table 4-1 Examples of barriers.

Barriers related to threats and susceptibility	Barriers related to coping capacity and consequences
• Enhanced condition monitoring of critical components • Vegetation management is adequate • The N-1 criterion is fulfilled • Adequate dimensioning criteria are available • Protection settings are tested	• Equipment for repair is available • Spare parts are standardised and available • Crew is available for restoration/repair • Reserve supply units are available • Communication systems are available

The consequences of power system failures can, for instance, be quantified and classified according to the amount of disconnected load (i.e., interrupted power) and stipulated average (weighted) duration, cf. Figure 2-1. Figure 4-3 gives an example of a consequence diagram using the two dimensions disconnected load and average duration for some blackouts in the past [8, 9, 31]. The figure also shows an example of the classification of consequences from minor to catastrophic as defined by [9]. This classification will depend upon the system or area under study. The disconnected load-dimension will typically be scaled down for a small city compared to a large city, for a local area compared to a region of a country, and so on. Thus, the term wide-area interruption or blackout is a relative term depending on the size of an area, a city or a community, cf. examples in Chapter 2, Figure 2-1.

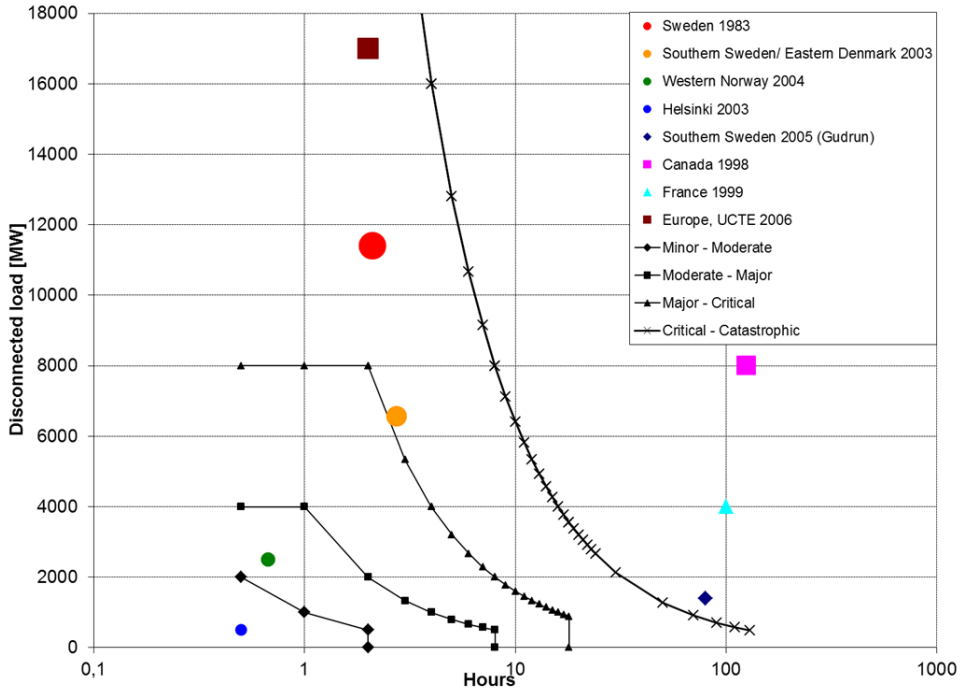


Figure 4-3 Consequence diagram, based on [8, 9].

There are two groups of events shown in Figure 4-3. Events in the first group to the left are typically initiated by technical or operational failures causing interruptions of limited duration but varying size in terms of load and area affected. The second group to the right consists of events where natural hazards (wind, icing) have caused wide geographical area damages to power lines resulting in comprehensive repair and extremely long durations [31].

4.2.2 Risk and vulnerability analysis framework for extraordinary events

Risk is defined as a combination of the probability of an event to occur, and its consequence [47, 48]. For some unwanted events it might be feasible to estimate the probability (or frequency) of occurrence, and further the risk. Figure 4-4 gives an example of a risk diagram where risk is plotted for the unwanted events in Figure 4-3 where information is available about the expected frequency of the event [41]. In this figure, the two dimensions of the consequence are combined into energy not supplied (MWh). The figure shows that even though two of the events have critical consequences (Figure 4-3) the risk is moderate due to the infrequent occurrence (low probability).

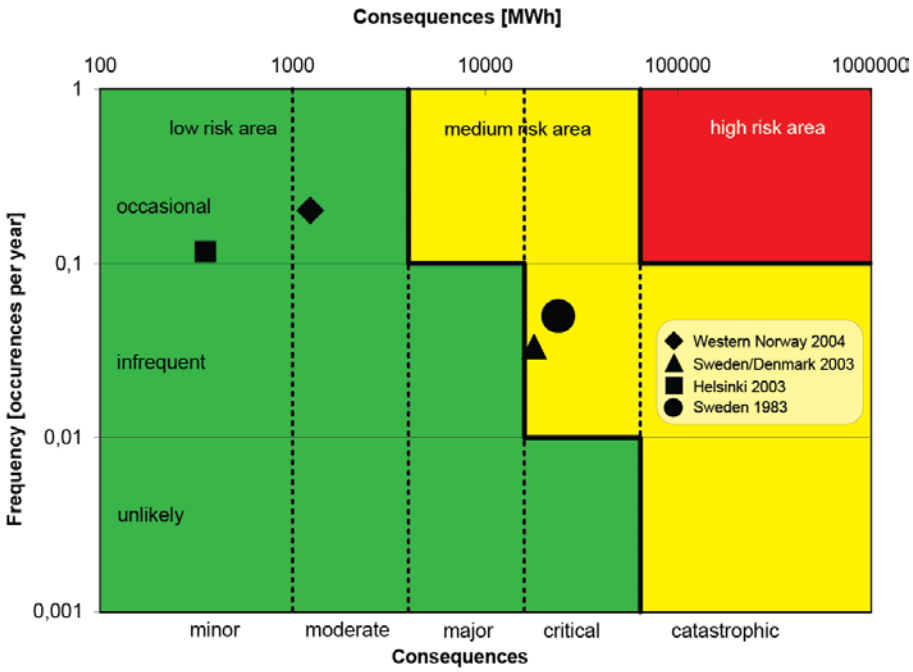


Figure 4-4 Risk diagram based on [31, 41].

Working with high impact, low probability (HILP) events, risk diagrams are not always appropriate as the consequence might still be unacceptable even if the risk is medium/low. Additional evaluations may therefore be necessary.

In risk and vulnerability analysis of electric power systems, a major challenge is to identify chains of events which could lead to wide-area interruptions and to determine the consequences of these events. The electricity system is an extremely complex and comprehensive infrastructure. The number of system states increases exponentially by 2^n for a system of *n* components that are typically assumed to be in one of two possible states ("up" or "down"). For a real system the number of system states will "explode" and it is a demanding task to analyse all possible system states. Due to a variety of vulnerability and risk influencing factors, as well as the complexity and size of the problem there is no single methodology suitable for an all-encompassing risk and vulnerability analysis of electricity supply [31, 56, 57].

The traditional risk analysis is typically performed according to the following main steps [9, 57]:

- Identification of threats and unwanted events
- Description of causes and probabilities (causal analysis)
- Classification of consequences (consequence analysis)
- Risk and vulnerability evaluation.

Previous studies indicate that there is no single methodology covering all these aspects, suitable for power system risk and vulnerability analysis of extraordinary events [56]. There is a need to combine different quantitative and qualitative methods. Examples of methods, supporting the different steps, are shown in Figure 4-5. The listed methods are regarded as the most relevant based on literature studies as well as experience from former work [9, 56-58]. This is further elaborated in [57]. See also Appendix A.3 for more detailed lists of relevant methods.

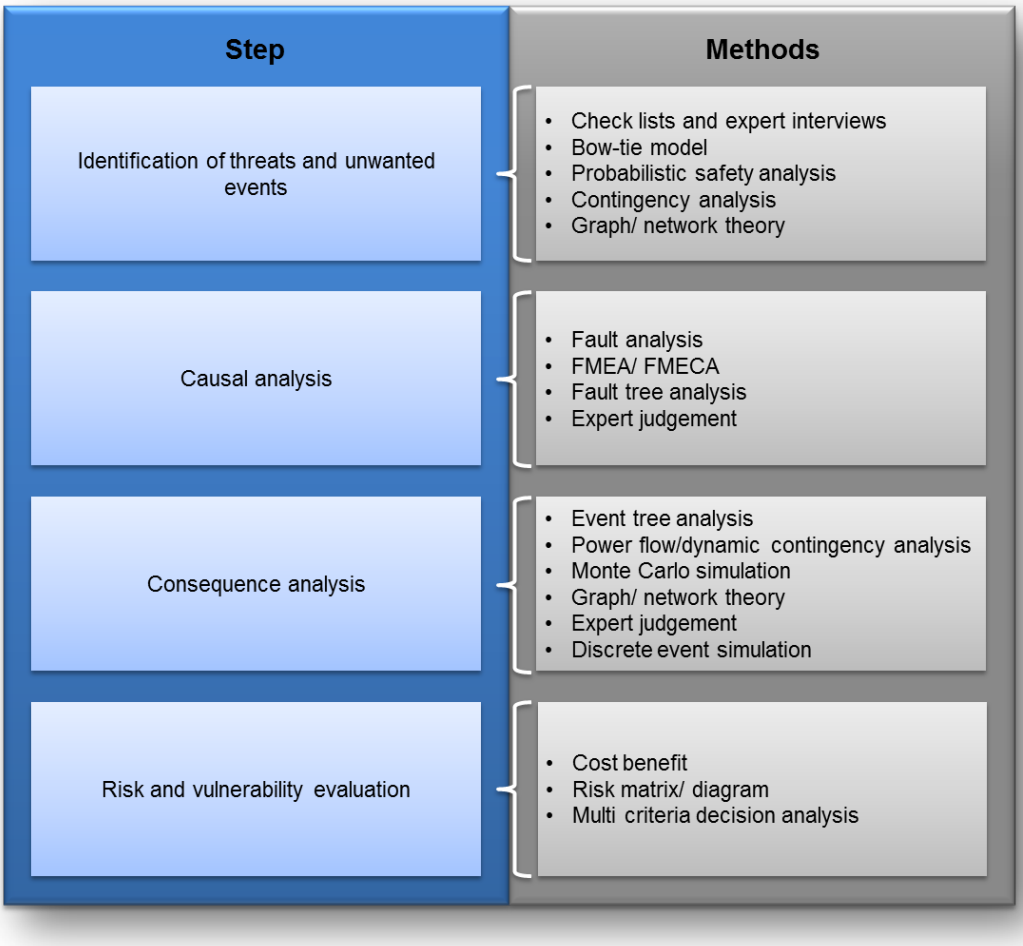


Figure 4-5 Risk and vulnerability analysis – possible methods, based on [57].

4.2.3 Identification of vulnerability

The traditional risk analysis typically starts early in the course of events that may lead to an unwanted event focusing on identification of threats and unwanted events [31]. The vulnerability analysis focuses less on the causes and is more concerned with the vulnerabilities that may cause disturbances in a system to result in the unwanted event and further result in severe consequences.

Vulnerability is in this report related to extraordinary events in the power system caused by power system failures. It is therefore important to identify critical outages, assets, locations and operating states, potentially leading to extraordinary events when the power system is exposed to threats. While the criticality dimension of vulnerability in Figure 3-1 refers to the consequences for the end-users (society), the term critical here refers to elements or aspects with potentials for severe consequences, i.e., factors being significant for the security of electricity supply. These factors give important information about vulnerability and input to the choices regarding development of indicators.

Critical outages, locations etc., will depend on different conditions varying among the grid operators. The critical factors must be identified by each operator through a risk and vulnerability analysis using tools like preliminary hazard analysis, contingency analysis and brainstorming/ expert evaluation.

The framework for vulnerability analysis proposed in the project is illustrated in Figure 4-6. It is proposed to use the bow tie model as a starting point. To be able to deal with extraordinary events, experiences show that it might be important to start with the consequences at the right hand side of the bow tie. When the critical consequences are identified, the next step is to identify the outages that may lead to these consequences. The following step is to identify the threats that may lead to these outages, before vulnerabilities are identified on both sides of the bow tie. Various factors influencing the coping capacity are identified as well, and finally a vulnerability evaluation is made identifying the existing and, even more important, any missing barriers against critical outages. These steps are further detailed in the following paragraphs.

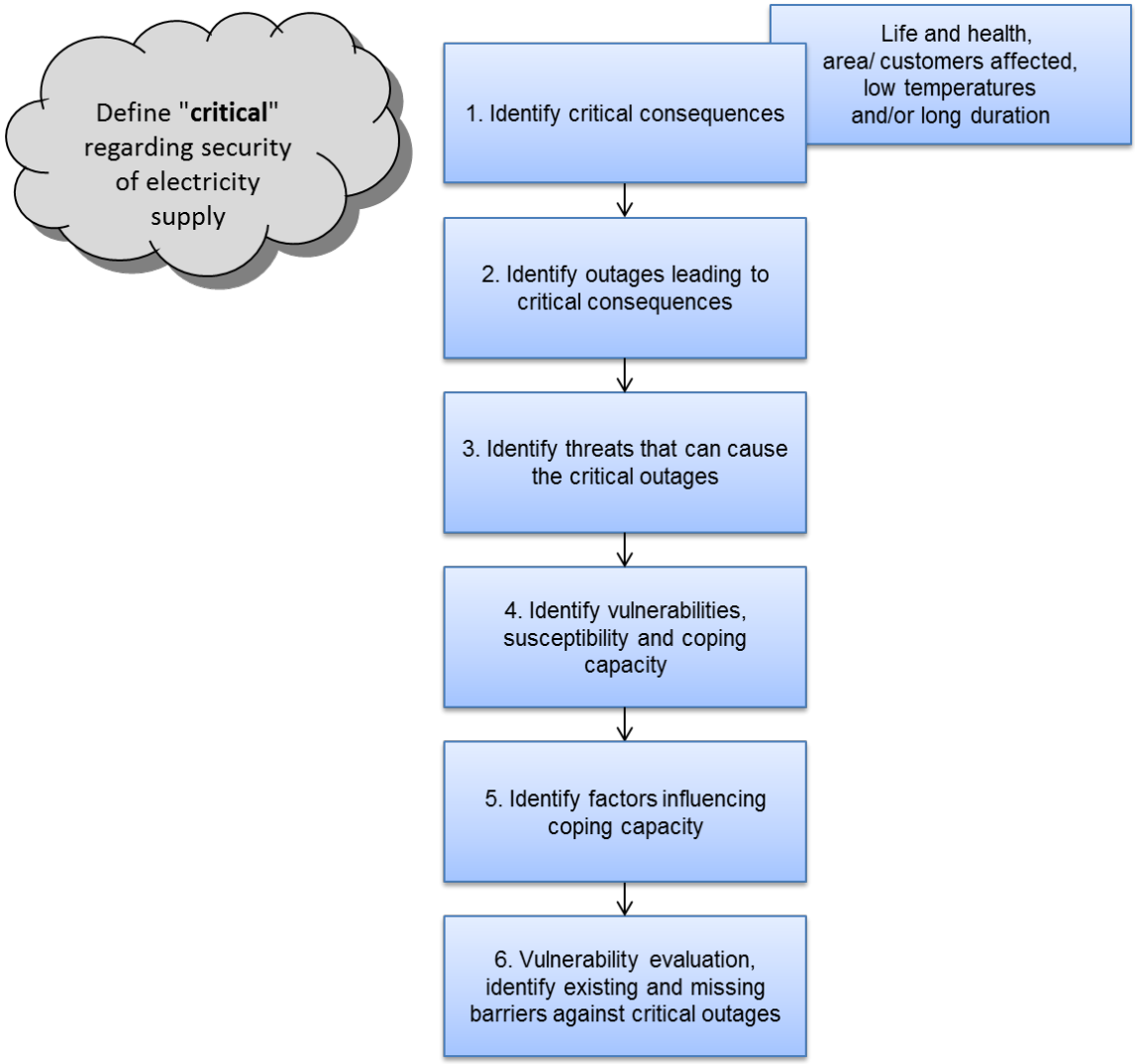


Figure 4-6 Vulnerability analysis methodology.

Step 0: Define "critical"
Before any vulnerability analysis process can start, it is necessary to define the term *"critical"*. This means that the grid operator must consider how to define critical consequences within their system with regards to security of electricity supply. This will be individual for each grid operator's supply area and can be stated, e.g., as a combination of lost load (MW) and duration (h) and may also depend on which part(s) of the network/ customers that are affected. The grid operator may need to co-operate with local authorities to be able to identify customers with critical loads, where e.g., life and health is at stake, etc.

Step 1: Identify critical consequences
In the first step of the analysis, critical consequences within the grid operator's supply area are identified, including any dependent infrastructure(s). Critical consequences are related to interruption of power supply to critical loads defined in step 0. The criticality of consequences is highly dependent on the area that is affected by loss of power supply, the number and type of customers affected, time until power supply is restored, as well as external factors like temperature and weather conditions.

Step 2: Identify outages leading to critical consequences
In the second step the component outages that can lead to critical consequences are identified. This step should also comprise identification of any critical locations and operating states. This means identifying events that lead to the critical consequences identified in step 1. Examples of such events are:

- Single or multiple outages, including common mode events, of systems or components
- Critical operating states where the demand cannot be covered
- Incidents or intended acts at critical locations:
    - Nodes in the network where infrastructures meet
    - Locations where, e.g., several cables are in the same right of way like under bridges, etc.

Step 3: Identify threats that can cause the critical outages
In the third step, threats that can cause the critical outages or threaten the critical locations are identified. All categories of threat; nature, human, operational, are covered. An example can be an area particularly exposed to weather (wind, icing), or digging activity.

Step 4: Identify vulnerabilities, susceptibility and coping capacity
In the fourth step susceptibilities and coping capacities are identified. This means identifying how the critical outage (unwanted event) can happen and why the consequences of the outage become critical. This step is closely related to the existing barriers related to susceptibility (preventing the critical outage) and coping capacity (limit the consequences of the critical outage).

Step 5: Identify factors influencing coping capacity
In the fifth step any factors that might hinder the coping capacity are identified. Examples of such factors are competence and resources/ preparedness, traffic jam, bad weather, and access to other infrastructures like telecommunications and roads.

Step 6: Vulnerability evaluation, identify existing and missing barriers against critical outages
In the sixth step a vulnerability evaluation is carried out, focusing on missing barriers related to susceptibility and coping capacity. This means identifying how the vulnerability of the system can be reduced, by introducing barriers aiming to prevent critical outages and/ or to reduce the consequence of critical outages.

Methods suitable for the various steps of the analysis regarding extraordinary events are listed in Appendix A.3.

4.3 Vulnerability indicators

In order to describe and monitor vulnerability and risk related to extraordinary events there is a need for indicators providing information about threats, susceptibility, coping capacity, potential consequences and barriers. The framework for development of vulnerability indicators is based on the concept of vulnerability described in Chapter 3 and the analysis methodology described in the previous section. The description in this section is partly based on or taken from [43, 46, 59].

4.3.1 Different types of indicators

Indicators can be defined as observable measures that provide insights into a concept or a system that is difficult to measure directly [60]. Vulnerability indicators should address different aspects regarding the vulnerability and cover both the susceptibility and coping capacity. However, vulnerability can only be seen in relation to threats. Thus, vulnerability indicators should also cover threats that the system is exposed to. Finally, the criticality for society has to be considered to assess the potential of severe consequences. All these aspects are important to give a complete picture of the vulnerability of the system. Therefore, vulnerability indicators are here understood as indicators which give information about the susceptibility and coping capacity and thus give insight into the risk related to extraordinary events.

There exist a wide range of categorizations of indicators. Safety indicators are mainly in focus in the literature, but it can be assumed that the types used for safety indicators can be applicable also for vulnerability indicators. The following categorization is regarded appropriate for the development of vulnerability indicators in this project [61]:

- Outcome versus activity based indicators
- Leading versus lagging indicators

Outcome and activity indicators monitor specific activities which are undertaken to reduce vulnerability. Outcome indicators give information if or not the desired result is achieved, while activity indicators are defined as means for measuring actions or conditions that should maintain or lead to improvements in safety [60].

Lagging and leading indicators refer to the state of vulnerability and risk (in our case related to extraordinary events):

- Lagging indicator: Information about the current vulnerability and how it has been in the past.
- Leading indicator: Information about how the vulnerability will develop in the future.

Leading indicators are closely related to activity indicators and lagging indicators are closely related to outcome indicators. Considered on a time scale, lead indicators will typically precede lag indicators. Examples of the different types of indicators are given in Table 4-2 using the technical condition of a power line as an example. Activity and outcome indicators are used for monitoring activities and their efficiency to reduce vulnerability as for example the number of replaced joints and the related power line faults.

Table 4-2 Examples of different types of vulnerability indicators [46].

Lagging	Leading	Activity	Outcome
Technical condition of power line	Prognosis for technical condition of power line based on an ageing model	Number of replaced joints of poor quality	Reduction in number of power line faults related to joints

Information about the technical condition of the components is a lagging indicator since it only provides information about the vulnerability at the moment the data was collected. However, it is possible to establish a leading indicator based on this data if it is used in an ageing model to estimate the development of the technical condition over time. This would give information about how the vulnerability could develop in the future. The number of poor quality joints that are replaced is an activity indicator since it measures the activity directly. It is often challenging to find an adequate outcome indicator related to the activity. A possible outcome indicator for the replacement could be the reduction in number of power line faults caused by joints of poor quality.

4.3.2 Indicators in use today

As described in Chapter 2, fault statistics is probably the best available data basis for documenting the security of supply regarding causes of power system failures and consequences in terms of interruptions. Figure 4-7 shows examples of indicators in use today based on the fault statistics. Fault frequency describes the result of exposure to threats and the susceptibility towards these threats. Energy not supplied (ENS) adds information about the coping capacity, i.e., the consequences of the unwanted event measured as interrupted load and duration. Expected interruption costs (EIC) add information about the societal consequences for different end-users.

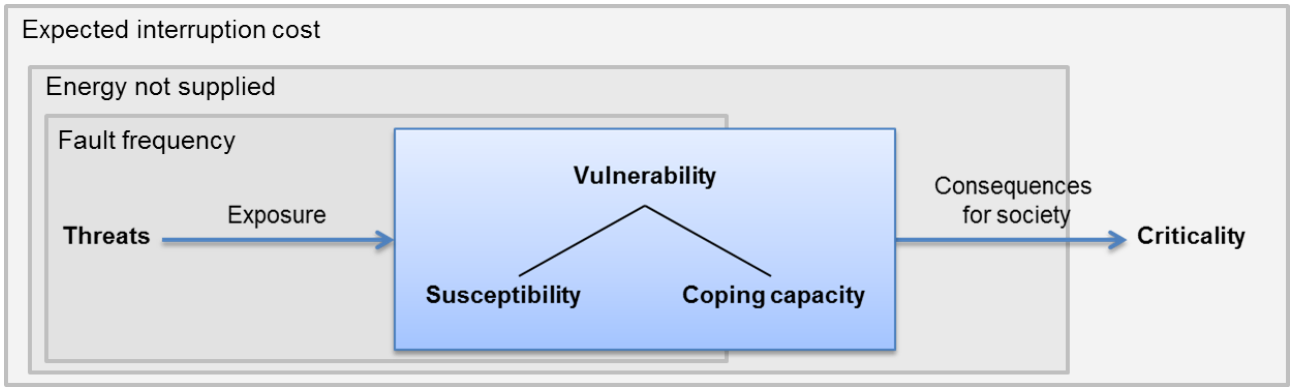


Figure 4-7 Examples of indicators describing parts of vulnerability [59].

In Norway, data about faults on components and interruptions of power supply to end-users, energy not supplied (ENS), Cost of Energy Not Supplied (CENS) [7], etc. CENS represents in principle the EIC indicator as described above. This data is collected using the Norwegian standard FASIT for collecting and reporting reliability data [44]. Data about faults and interruptions for all voltage levels 1 – 420 kV has been continuously reported in Norway for the last 23 years 1989 – 2011. In this project, this data is analysed, grouped and compared to reveal main causes, trends, etc. Extensive results are presented in the report [62]. Figure 4-8 and Figure 4-9 show examples of the available statistics. Energy not supplied (ENS) for the period 1989 – 2011 at all high voltage levels 1 – 420 kV is shown in Figure 4-8. The figure shows ENS divided in notified and not notified interruptions, including and excluding the New Year Day storm in 1992 and the storm Dagmar in 2011. Figure 4-9 shows the fault frequency for the total number of faults on the voltage levels 1 – 22 kV and 132 kV respectively, for the ten year period 2002 – 2011.

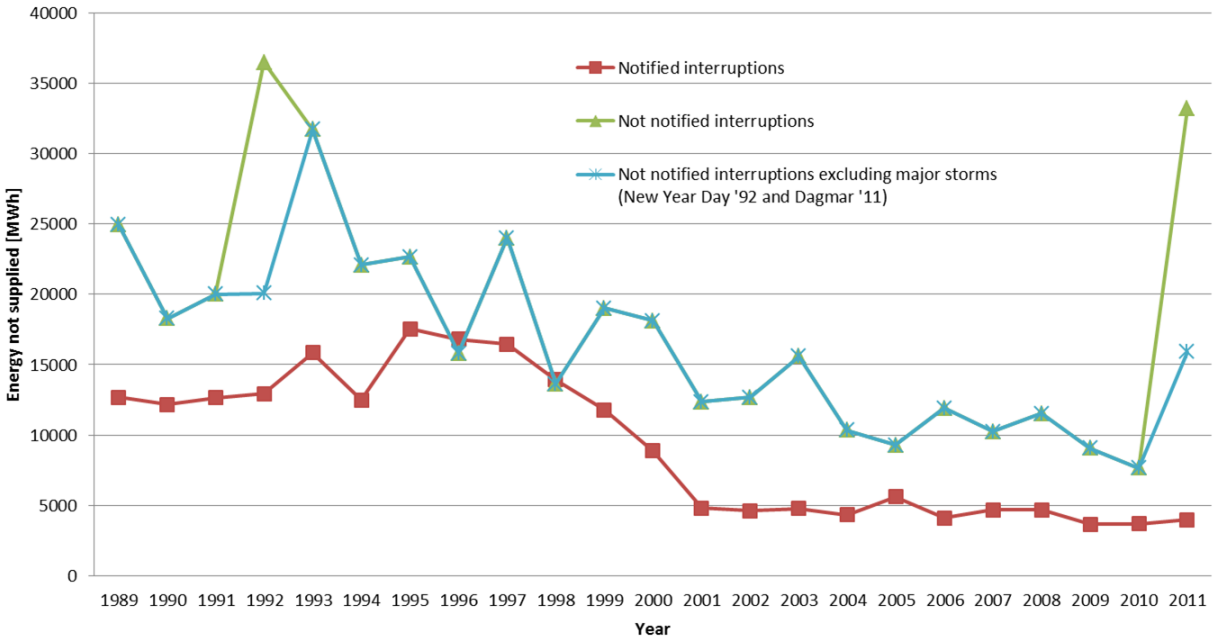


Figure 4-8 Energy not supplied 1989 – 2011 in Norway, divided in notified and not notified interruptions [62].

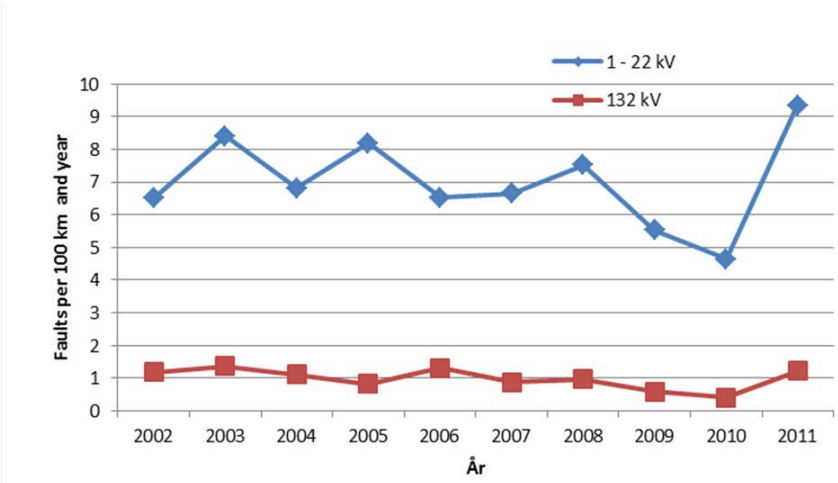


Figure 4-9 Fault frequency for power lines in Norway, 1 – 22 kV and 132 kV, 2002 – 2011 [62].

There has been a considerable decrease in ENS over the 23 year period. However, ENS was double in 2011 compared to the average on the previous ten year period, due to the storm Dagmar which alone caused about 17 GWh [17]. Similarly, a significant increase in the fault frequency in 2011 can be observed in Figure 4-9, for both MV and regional power lines. Here, it should be mentioned that a standardized method for estimation of ENS was introduced in 2000 and the CENS arrangement was put into force in 2001. The main failure cause in Norway is natural hazards (wind, vegetation, icing, etc.) accounting for a little less than 50 % of the disturbances, while the same group of causes counts for more than 50 % of ENS.

Fault frequency, ENS and EIC are lagging indicators describing past performance. They give aggregate information about vulnerability. However, as mentioned above there is a need for indicators providing information about each of the dimensions; threats, susceptibility, coping capacity and potential consequences. Obviously the above mentioned indicators are inadequate for the purpose of monitoring the various dimensions of vulnerability, since too many effects are aggregated.

Fault frequency might be a more useful indicator of the susceptibility if it is possible to divide the faults in different classes of causes (threats). But, data from the fault statistics only contains information about the current components and those that have failed, in the current system and conditions. In addition, there is a need for leading indicators capable of predicting the development of the vulnerability. Such leading vulnerability indicators are requisite to provide information about risk exposure related to extraordinary events in a changing power system.

4.3.3 Framework for development of vulnerability indicators

After having defined what is meant by vulnerability and identified the purpose and need for indicators, the next step is to find suitable indicators to cover the relevant aspects of vulnerability according to the analysis framework presented above and for the given purpose. Checklists and criteria should be developed for the evaluation of proposed indicators. Subsequent steps are collecting the necessary data to establish the indicator as well as defining appropriate units, scales and calculation methods for documenting the indicators. The framework regarding indicator development process and evaluation criteria is thoroughly described in [63].

Vulnerability indicators are supposed to cover the internal and external dimensions according to Figure 3-1 and in principle there is one set of indicators for each identified threat. Based on case studies as reported in e.g., [24, 55] examples of possible indicators can be established. The framework and examples in qualitative terms are summarized in Figure 4-10.

In the upper part of Figure 4-10, it is shown that the starting point is the risk and vulnerability analysis to identify critical outages, assets, locations and operating states, i.e. those critical for the security of electricity supply, as described in Section 4.2 This analysis is a prerequisite for the choice of indicators to be developed, to enable monitoring of vulnerabilities related to extraordinary events.

In the lower left part of Figure 4-10, examples of threat indicators are given for the major threat categories: natural hazard, technical/operational and human errors. Weather prognosis of wind, snow and icing parameters will be relevant indicators for weather related threats for instance in Norway. The loading degree of components and system gives information about operational stress/threats, while construction work such as digging activity in an area is an indicator of threats related to human errors. Regarding susceptibilities, technical condition of the identified critical components as well as competence on condition evaluation is emphasized. Competence on system analyses like risk and vulnerability analysis is in itself also an indicator of susceptibility.

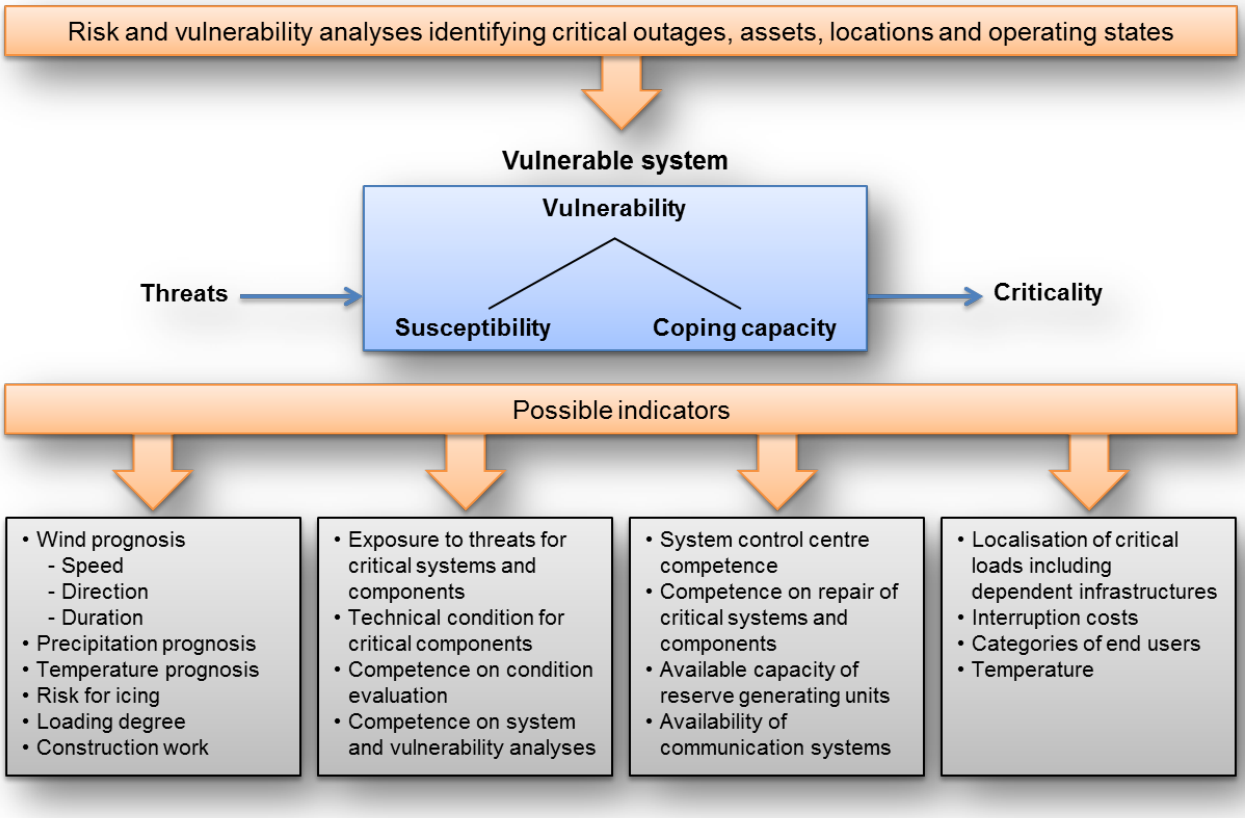


Figure 4-10 Framework and examples of vulnerability indicators [59].

Possible coping capacity indicators are related to the available competence for repairing critical components and systems as well as the available resources and equipment for restoration. Indicators for threats specifically against the coping capacity such as weather conditions or traffic problems are not shown the figure.

The figure also shows examples of indicators describing the criticality of the end-users in terms of localization of critical loads including dependent infrastructures, interruption costs and categories of end-users as well as temperature. These factors are to a large extent independent of a specific threat. The same is true for coping capacity except when it comes to competence on and spare parts for affected critical components.

The indicators in Figure 4-10 are general examples. Network companies will need to develop more specific indicators that should be associated with the types of threats the network is exposed to and the related vulnerabilities. More examples are given in [63].

4.4 Case studies and analyses of extraordinary events

In this project, analyses are performed of extraordinary events (wide-area interruptions, blackouts) that have occurred in the past. The purpose has been to learn from past events about vulnerabilities, i.e., susceptibilities and coping capacities, the causal relationships to threats, the course of events and the consequences. The analyses have helped to identify vulnerabilities, not only for providing examples, but also in the structuring and the development of the vulnerability framework. In addition, the project provides analyses of the fault and interruption data collected on a national basis in Norway, from the standardized system FASIT [44]. These analyses give lagging information about security of electricity supply (in terms of reliability), i.e., about fault frequency, energy not supplied and costs of energy not supplied as shown in Figure 4-7, as well as the main causes (threats), the main components that have failed, etc.

The case studies of historic events are structured according to the analysis framework using the bow tie model to identify threats, vulnerabilities, barriers and consequences. As such, the studies give examples of vulnerability analyses. Possible vulnerability indicators are described in qualitative terms like those presented in Figure 4-10, for the different dimensions of vulnerability (cf. Figure 3-1). These case studies comprise amongst other the Steigen and Oslo S events shown in Figure 2-1, the power supply to the small island Leka in the middle of Norway, the strained power situation to the BKK area in the Western part of Norway, the Europe blackout in 2006 [64] and the storm Dagmar in Norway, Sweden and Finland in 2011 [17]. More information about these case studies can be found in [17, 24, 59].

In addition, case studies were carried out in cooperation with two network companies participating in the project. The purpose of these case studies was to provide a foundation for the framework for development of vulnerability indicators described in [63] and for the vulnerability analysis methodology as described in Section 4.2. The aim in these studies was to develop vulnerability indicators for power lines in the MV distribution and regional grids, in quantitative terms, using available data at the network companies. The studies, which emphasized the susceptibility 'technical condition of power lines' to weather exposure and corresponding coping capacity, are thoroughly described in [63, 65].

4.5 Workshops, seminars and co-operation

This research project has co-operated with academic partners from various disciplines such as power system security and reliability analysis, fundamental risk and vulnerability methodology, societal security and critical infrastructures, and social sciences. The main Norwegian partners have been as follows:

- Norwegian University of Science and Technology (NTNU)
  - Department of Electric Power Engineering
  - Department of Production and Quality Engineering
  - Department of Interdisciplinary Studies of Culture
  - Department of Psychology
  - NTNU Social Research, Studio Apertura
- SINTEF Technology and Society, Safety Research.

The project has benefited from national co-operation within ROSS Gemini Centre[3] and cross disciplinary knowledge-building projects funded by the Research Council of Norway, such as: DECRIS (Risk and Decision Systems for Critical Infrastructures)[4] and CISS (Critical infrastructures, public sector

[3] ROSS Gemini centre: Reliability and Safety Studies at NTNU / SINTEF, http://www.ntnu.edu/ross
[4] More information about the DECRIS and CISS projects can be found at: http://www.sintef.no/samrisk

reorganization and societal safety), within the societal field in the SAMRISK programme. In addition, the project has co-operated with the knowledge-building project Integration of methods and tools for security of electricity supply analysis, within the field of electric power systems in the RENERGI programme.

The international co-operation in this project has served several purposes; competence building and quality assurance in the research work, as well as network building for future co-operation in projects related to security of electricity supply, e.g., in EU 7th FP for research. The international partners involved in the project were:

Lund Institute of Technology (LTH, PhD Jonas Johansson)
- LUCRAM (Lund University Centre for Risk Analysis and Management)
- Societal security, interdependencies, risk and vulnerability analysis

University of Manchester (Prof. Daniel Kirschen, now at University of Washington)
- Probabilistic modelling of catastrophic events in power systems
- Techniques for quantifying risks in power systems

Aalto University School of Electric Power Engineering (Prof. Liisa Haarla)
- Power system security and reliability analysis

University of Saskatchewan (Prof. emeritus Roy Billinton, Prof. Rajesh Karki)
- Power system reliability methodologies

Additional arenas for networking in Europe
- European Association of Research and Technology Organizations (EARTO) / EuroTech Energy Working Group
- EU 7FP projects (call texts, relevant projects, applications)
- European Energy Research Alliance (EERA) Joint Programme (JP) Smart Transmission, contributions
- European Electricity Grid Initiative (EEGI) roadmap contributions.

The international co-operation has taken place through workshops, seminars, discussions, co-operation between PhD-students, contributions to call texts, input to research project applications, etc., as described in the introduction to Chapter 4.

Workshops – topics (including national workshop):
- Scenarios for vulnerabilities in a changing power system, with project partners, Trondheim February 2009
- Vulnerability and reliability analysis methods, with Prof. emer. Roy Billinton, Oslo September 2009
- From traditional reliability analysis of electric power systems to risk analysis of extraordinary events, with international project partners, Trondheim October 2009
- Reliability analysis methodology in the context of security of electricity supply analysis, project-internal, Trondheim April 2010
- Technical condition of the power grid, project-internal, Trondheim June 2010
- Vulnerability and reliability analysis methods and extraordinary events, with PhD Jonas Johansson (LTH), in co-operation with the knowledge-building project Integration of methods and tools for security of electricity supply analysis, Trondheim December 2010
- Vulnerability indicators, with project partners, Gardermoen February 2011
- Risk of extraordinary events and analysis methods, with the RCAM group at KTH Royal Institute of Technology, Trondheim March 2011
- Organizational vulnerability indicators, ROSS Gemini centre, Trondheim June 2011
- Vulnerability indicators for power lines, project-internal, Trondheim February 2012
- Critical infrastructures and societal security, ROSS Gemini Centre, Trondheim October 2012

The project has also arranged three workshops in the EARTO/EuroTech Energy Working Group, on the topic security of electricity supply. This group consists of the following research institutes: TECNALIA, VTT, FOI (Swedish Defence Research Agency), JRC, Fraunhofer, QinetiQ, TNO and SINTEF Energy Research. The group worked together in 2009 – 2010 with the aim to influence EU-policies and strategic research agendas regarding security of electricity supply, see [26]. The collaboration resulted in input to the work programme of EU 7 FP, Area ENERGY and call texts. Later, the work is partly followed up in EERA JP Smart Transmission [53].

The project has arranged two seminars in Norway:

- SINTEF seminar: "Without electricity in the aftermath of next storm?" (In Norwegian: "Uten strøm også etter neste storm?"), Oslo 19 April 2012
- "The Vulnerability project – overview and main results" (In Norwegian: "Sårbarhetsprosjektet – presentasjon og diskusjon av resultater"), Oslo 29 April 2013

In addition to workshops and seminars, the project results have been presented in international conferences, published in scientific journals and included in various presentations at workshops, seminars and conferences. The project has served as basis for discussion and co-operation for several PhD projects. The main publications and presentations are listed in Section 4.6 and Appendix A.2.

4.6 Publications

4.6.1 Technical reports

There are four technical reports describing main results from the project:

Vulnerability in electric power grids. State of the art and framework for vulnerability indicators
Matthias Hofmann, Oddbjørn Gjerde, Gerd H Kjølle
SINTEF Energy Research, December 2011, TR A7120

Vulnerability indicators for electric power grids
Matthias Hofmann, Gerd H Kjølle, Oddbjørn Gjerde
SINTEF Energy Research, June 2013, TR A7276

Vulnerability and security in a changing power system. Executive summary (this report)
Gerd H Kjølle, Oddbjørn Gjerde, Matthias Hofmann
SINTEF Energy Research, June 2013, TR A7278

Analyses of faults and interruptions in the electric power grid 1989 – 2011
(In Norwegian: Analyser av feil og avbrudd i kraftnettet 1989 – 2011)
Gerd H Kjølle, Ruth Helene Kyte, Hanne Vefsnmo, Jostein Lille-Mæhlum
SINTEF Energy Research, April 2013, TR A7279

4.6.2 Journal and conference papers

This section gives an overview of papers produced in the project, the most recent publications from the top of the list. Appendix A.2 lists the presentations, posters and project memos provided by the project.

Gerd Kjølle, Ruth Helene Kyte, Matz Tapper, Kenneth Hänninen:
Major storms – Main causes, consequences and crisis management
CIRED 2013, Stockholm, 10 - 13 June 2013

Matthias Hofmann, Oddbjørn Gjerde, Gerd H Kjølle, Eivind Gramme, Johan G Hernes, Jan A Foosnæs:
Developing indicators for monitoring vulnerability of power lines – case studies
CIRED 2013, Stockholm, 10 - 13 June 2013

Gerd H Kjølle:
The electricity system of the future (SmartGrids) and security of electricity supply
ROSS Gemini Centre, SINTEF report A24477, June 2013, pp. 18 - 19

Emil Hillberg, Jarno Lamponen, Liisa Haarla, Ritva Hirvonen:
Revealing stability limitations in power system vulnerability analysis
MEDPOWER - Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion, Cagliari, October 2012

Gerd H Kjølle, Ruth Helene Kyte:
Dealing with major storms in asset management
NORDAC 2012, Helsinki, September 2012

Emil Hillberg, Frode Trengereid, Øyvind Breidablik, Kjetil Uhlen, Gerd H Kjølle, Stig Løvlund, Jan Ove Gjerde:
System Integrity Protection Schemes – Increasing operational security and system capacity
CIGRE Session 2012, Paris, August 2012

Gerd H Kjølle, Oddbjørn Gjerde, Matthias Hofmann:
Monitoring vulnerability in power systems. Extraordinary events, analysis framework and development of indicators
PMAPS 2012, Istanbul, June 2012

Matthias Hofmann, Gerd H Kjølle, Oddbjørn Gjerde:
Development of indicators to monitor vulnerabilities in power systems
PSAM11/ESREL2012, Helsinki, June 2012

Ruth Helene Kyte, Gerd H Kjølle:
When extreme weather hits the power grid (In Norwegian: Når ekstremvær rammer kraftnettet)
Energiteknikk nr. 3, April 2012

Emil Hillberg, Trond Toftevaag:
Equal-area criterion applied on power transfer corridors
IASTED Asian Conference on Power and Energy Systems, April 2012

Gerd H Kjølle, Ingrid B Utne, Oddbjørn Gjerde:
Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies
Reliability Engineering and System Safety 105, pp. 80 – 89, September 2012

Emil Johansson, Kjetil Uhlen, Gerd H Kjølle, Trond Toftevaag:
Reliability evaluation of wide area monitoring applications and extreme contingencies
PSCC - 17th Power Systems Computation Conference, Stockholm, 22 - 26 August 2011

Oddbjørn Gjerde, Gerd H Kjølle, Nina K Detlefsen, Geir Brønmo:
Risk and vulnerability analysis of power systems including extraordinary events
IEEE PES, Powertech, Trondheim, 19 - 23 June 2011

Oddbjørn Gjerde, Gerd H Kjølle, Johan G Hernes, Birger Hestnes, Jan A Foosnæs:
Indicators to monitor and manage electricity distribution system vulnerability
CIRED 2011, Frankfurt, 6 - 9 June 2011

Emil Johansson, Kjetil Uhlen, Gerd H Kjølle:
Mitigating extraordinary events using wide area monitoring applications
CIGRE Symposium Recife, 3 - 6 April 2011

Gerd H Kjølle, Oddbjørn Gjerde, Matthias Hofmann, Birger Hestnes, Johan G Hernes:
Can vulnerabilities in power grids be monitored? Is it possible to find relevant indicators for the purpose? (In Norwegian: Kan sårbarheter i kraftnettet overvåkes? Er det mulig å finne gode indikatorer for dette?)
NEF Teknisk møte, Trondheim, 24 - 25 March 2011

Gerd H Kjølle, Oddbjørn Gjerde:
Integrated approach for security of electricity supply analysis
International Journal of System Assurance Engineering and Management, Vol.1, Issue 2, 2010

Emil Johansson, Kjetil Uhlen, Agnes Nybø, Gerd H Kjølle, Oddbjørn Gjerde:
Extraordinary events: Understanding sequence, causes and remedies
ESREL, Rhodes, 6 - 10 September 2010

Gerd H Kjølle, Ingrid B Utne:
Critical infrastructures and risk analysis of electricity supply
ESREL, Rhodes, 6 - 10 September 2010

Agnes Nybø, Gerd H Kjølle, Kjell Sand:
Vulnerability in power systems - the effect of maintenance and reinvestments
NORDAC, Ålborg, 6 - 7 September 2010

Gerd H Kjølle, Oddbjørn Gjerde, Agnes Nybø:
A framework for handling high impact low probability (HILP) events
CIRED Workshop, Lyon, 7 - 8 June 2010

Gerd H Kjølle:
Critical infrastructures and societal security (In Norwegian: Kritiske infrastrukturer og samfunnssikkerhet), Xergi nr. 3 – February 2009

Gerd H Kjølle:
Vulnerability in the electricity supply and emergency preparedness (In Norwegian: Sårbarhet i kraftforsyningen og beredskap), Xergi nr. 3 – February 2009

4.6.3 Book chapters

The project has contributed to three book chapters in the following books:

P. Hokstad, I. B. Utne, J. Vatn (eds.), Risk and Interdependencies in Critical Infrastructures, Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2 (Online), ISBN: 978-1-4471-4660-5 (Print), Springer-Verlag London 2012

Gerd Kjølle and Oddbjørn Gjerde:
Book chapter 7: Risk analysis of electricity supply, pp. 95-108

Oddbjørn Gjerde and Gerd Kjølle:
Book chapter 8: Risk of electricity supply interruptions, pp. 109-125

R. Billinton, A. K. Verma, R. Karki (eds.), Reliability Modeling and Analysis of Smart Power Systems, Springer Series in Reliable and Sustainable Electric Power and Energy Systems Management, in press 2013

Vijay Venu Vadlamudi, Rajesh Karki, Gerd H. Kjølle, Kjell Sand:
Book chapter: Reliability-Centric Studies in Smart Grids: Adequacy and Vulnerability Considerations

4.6.4 Doctoral (PhD) and master theses, NTNU

There has been one PhD candidate (Emil Hillberg) within this project on the topic "Models and methods for risk analysis of extraordinary events". The thesis of Emil Hillberg is entitled "Perception, Prediction and Prevention of Extraordinary Events in the Power System", to be completed in 2013.

The objective of the PhD project has been to develop models and methods to analyse the risk of extraordinary events for increased security and/or increased utilisation of the power system, focussing on the operation of the power system.

The scope of the work has been divided in three main areas:

- Perception of extraordinary events
  - Categorisation of events, analyses of causes, and identification of critical characteristics
- Prediction of extraordinary events
  - Identification of study requirements and development of a framework and methodology
- Prevention of extraordinary events
  - Development of methods to prevent extraordinary events.

A few master students at the Norwegian University of Science and Technology (NTNU) have worked on specialisation projects and master theses in relation to the project:

Hanne Bakken, Kristine Bjørndal Søndenaa, Karina Kojedahl Bjørkedal:
How can the SINTEF-project "Vulnerability and security in a changing power system" enable dissemination of research to the public? (In Norwegian: Hvordan kan SINTEF-prosjektet "Vulnerability and security in a changing power system" legge til rette for allmennrettet forskningsformidling?)
Specialisation project, NTNU, May 2010

Jannicke C Mørk:
Analyses of faults and interruptions in the power system in the BKK-area (In Norwegian: Analyser av feil og avbrudd i kraftsystemet i BKK-området)
Specialisation project, NTNU, December 2010

Jannicke C Mørk:
Reliability of supply and risk of blackout in the BKK-area (In Norwegian: Leveringspålitelighet og risiko for nettsammenbrudd i BKK-området)
Master Thesis, NTNU, June 2011

Karina K Bjørkedal:
An analysis of the media reach of Bergens Tidende and Aftenposten regarding the power line Sima – Samnanger (In Norwegian: Ei analyse av Bergens Tidende og Aftenposten si mediedekning av luftledninga Sima – Samnanger)
Specialisation project, NTNU 2011

Karina K Bjørkedal:
The media power of security of supply (In Norwegian: Forsyningssikkerheitas mediekraft – Ei kvantitativ analyse av Adresseavisen, Aftenposten og Bergens Tidende)
Master Thesis, NTNU, December 2011

Jostein Lille-Mæhlum:
Vulnerability indicators for power lines (In Norwegian: Sårbarhetsindikatorer for kraftledninger)
Specialisation project, NTNU, December 2012

Jostein Lille-Mæhlum:
Vulnerability and reliability of supply indicators for electric power grids (In Norwegian: Indikatorer for sårbarhet og leveringspålitelighet i kraftnett)
Master Thesis, NTNU, June 2013

5 Conclusions and recommendations

This report has presented the main results from the knowledge-building project Vulnerability and security in a changing power system, developed in collaboration with energy authorities and grid operators.

Society is increasingly dependent on a secure electricity supply to cover basic needs such as food and water supply, heating, safety, financial services, etc. At the same time, the power system is under change for a number of reasons, due to e.g., increased utilization of the power grids, integration of intermittent renewable generation, smart grids, and climate change. These factors may affect the vulnerability of the power system. Vulnerability is here defined as an internal attribute of the system and is divided in susceptibility and coping capacity towards a certain hazard or threat. It is essential to control the vulnerabilities in planning and operation of the power system. Dedicated vulnerability analyses as well as suitable indicators are necessary to measure how vulnerable the power system is. However, presently there are only few, if any, available indicators.

The project has focused on extraordinary events, i.e., wide-area interruptions or long-lasting interruptions with severe impact on society. Research results are obtained in three main areas. First of all, a framework is developed of definitions, indicators and methods that can be used to monitor and classify vulnerabilities in electric power grids. Different types of indicators are addressed to cover various dimensions of vulnerability and example indicators are discussed. Second, methods and tools for power system risk and vulnerability analysis of extraordinary events are developed and tested. The methods take the conceptual bow tie model as a starting point and different methods of risk and vulnerability analysis are utilised. Third, case studies are performed to illustrate the development and use of vulnerability indicators and methods. Several indicators are tested through case studies in co-operation with grid operators. In addition, historical blackouts and extraordinary events in power systems are analysed to learn from past events and to understand the course of action that led to these events.

The project provides knowledge that can contribute to a sound basis for a more socio-economic efficient operation and development of the transmission and distribution systems. In the vulnerability framework it is distinguished between ordinary (frequent) and extraordinary (infrequent, HILP) events. The knowledge basis serves a range of purposes for the different stakeholders, enabling:

- Risk and vulnerability analysis of transmission and distribution systems (regulated through the regulation of emergency preparedness in Norway)
- Identification and prioritization of risk and vulnerability reducing measures
- Evaluation on how to handle and control vulnerabilities to meet defined criteria
- Incorporation of vulnerability issues in the regulation and supervision of network companies
- Better decision making in planning and operation of the changing power system
- Better contingency and emergency preparedness planning.

The knowledge and network building in this project has already provided a basis for participation in EU-projects [54], giving potentials for increased added value for the participating companies.

The results from this knowledge-building project can be used as background in the development of specific indicators and methods that can be used by grid operators and energy authorities in planning and operation. The project recommends how to develop indicators and define methods, scales and the necessary data to be collected. A simple tool for vulnerability analysis is developed. Moreover, the project proposes a methodical way of learning from past events.

The project recommends further research and knowledge-building in two main areas: 1) Societal consequences of wide-area interruptions (criticality), society's needs and acceptance with regards to security of electricity supply. 2) Interdependencies in the power system and the integrated ICT system with regards to control system, new technologies and components, including new ways of operating the power system in the future (smart grids).

6 References

1. EU Commision, *On a European programme for critical infrastructure protection. Green Paper*. 2005: Brussels.
2. Kröger, W. and E. Zio, *Vulnerable Systems*. 2011, London: Springer.
3. DSB, *Nasjonal sårbarhets- og beredskapsrapport* in *NSBR*. 2011: Oslo.
4. EU Commision, *Concerning measures to safeguard security of electricity supply and infrastructure investment*. 2006.
5. Eurelectric, *Security of electricity supply*. 2004: Brussels.
6. OED, *Forskrift om leveringskvalitet i kraftsystemet*, in *FOR 2004-11-30 nr 1557*. 2004, Lovdata: Oslo.
7. Langset, T., et al., *Quality adjusted revenue caps – a model for quality of sup-ply regulation*, in *CIRED International conference & exhibition on electricity distribution*, CIRED, Editor. 2001: Amsterdam.
8. NordSecurEl, *Risk and vulnerability assessments for contingency planning and training in the Nordic electricity system. Final report*. 2009, Statens Energimyndighet Eskilstuna
9. Doorman, G., et al., *Vulnerability of the Nordic power system*, in *SINTEF Energi. Teknisk rapport TR A5962*. 2004, SINTEF Energi: Trondheim.
10. NVE, *Ny forskrift om energiutredninger. Oppsummering av høringsuttalelser og endelig forskriftstekst*, in *NVE. Rapport 65-2012*. 2012, Norges Vassdrags- og Energidirektorat (NVE): Oslo.
11. Statnett, *Systemdrifts- og markedsutviklingsplan 2012*. 2012, Statnett: Oslo.
12. NORDEL, *The Nordic Grid Code*, in *ENTSO-E, https://.www.entsoe.eu/*. 2007.
13. Johansson, E., et al. *Extraordinary events - understanding sequence, causes and remedies*. in *ESREL 2010*. 2010. Rhodes.
14. Bialek, J.W., *Blackouts in the US/Canada and continental Europe in 2003: Is liberalisation to blame?*, in *IEEE PowerTech*. 2005: St. Petersburg.
15. U.S.-Canada Power System Outage Task Force, *Final Report on the 2003 Blackout in the United States and Canada: Causes and Recommendations*. 2004.
16. UCTE, *System disturbance on 4 November 2006. Union for the co-ordination of transmission of electricity*, UCTE, Editor. 2007.
17. Kjølle, G. and R.H. Kyte, *Major storms – main causes, consequences and crisis management*, in *CIRED*, CIRED, Editor. 2013: Stockholm.
18. Statnett, *Analyse av driftsforstyrrelsen på Vestlandet 13. februar 2004*. 2004.
19. DSB, *Brann i kabelkulvert - Oslo Sentralstasjon 27.11.2007*. 2008, Direktoratet for samfunnssikkerhet og beredskap.
20. Hillberg, E., et al., *Power System Reinforcements - the Hardanger Connection.* ELECTRA, 2012(260): p. 4-15.
21. IEA, *Learning from the blackouts: Transmission system security in competetive electricity markets*. 2005, IEA: Paris.
22. Eurelectric, *Power outages in 2003 - Task force power outages*. 2004, Union of Electricity Industry.
23. Swedish Energy Agency, *Storm Gudrun - What can be learnt from the natural disaster of 2005?* 2007.
24. Kjølle, G., O. Gjerde, and A. Nybø, *A framework for handling high impact low probability (HILP) events*, in *CIRED Workshop*. 2010: Lyon.
25. Energi21, *Nasjonal strategi for forskning, utvikling, demonstrasjon og kommersialisering av ny energiteknologi*, Energi21, Editor. 2011, Norges forskningsråd: Oslo.
26. Dyken, S.v. and G. Kjølle, *State of the art regarding security of electricity supply on a European level*, in *SINTEF Energi. Arbeidsnotat*. 2011, SINTEF Energi: Trondheim. p. 47.
27. The European Electricity Grid Initiative (EEGI), *Roadmap 2010-18 and detailed implementation plan 2010-12*. 2010.
28. Statnett, *Nettutviklingsplan 2011*. 2011: Oslo.

29. NOU, *Når sikkerheten er viktigst - Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*, Norwegian CIP Commission, Editor. 2006, NOU: Oslo.
30. Kjølle, G., I.B. Utne, and O. Gjerde, *Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies.* Reliability Engineering & System Safety, 2012. **105**: p. 80-89.
31. Hokstad, P., I.B. Utne, and J. Vatn, eds. *Risk and interdependencies in Critical Intrastructures.* Springer series in Reliability Engineering. 2012, Springer: London.
32. EU Commision, *Proposal for a Regulation on "Guidelines for trans-European energy infrastructure".COM/2011/658*. 2011.
33. European Network of Transmission System Operators for Electricity, E., *Ten-year network development plan 2010-2020*. 2010.
34. Thema Consulting, *På nett med framtida. Kraftnettets betydning for verdiskaping*, in *Thema Rapport 2012-34*. 2013: Oslo.
35. International Risk Governance Council (IRGC), *Managing and reducing social vulnerabilities from coupled critical infrastructures.* 2007.
36. North American Electric Reliability Corporation (NERC), *Reliability Considerations from the Integration of Smart Grid*. 2010: Princeton.
37. Statnett, *Områder med redusert driftssikkerhet i sentralnettet*. 2011: Oslo.
38. NVE, *Annual Report 2011 The Norwegian Energy Regulator*, in *NVE-RAPPORT 19-12*. 2012: Oslo.
39. NVE, *Innstilling til OED - forslag til endring av energilovforskriften. Oppsummering av høringsuttalelser og endelig forskriftstekst*, in *NVE-RAPPORT 68-2012*. 2012: Oslo.
40. NVE, *Driften av kraftsystemet 2012*, in *NVE-RAPPORT 44 - 2013*. 2013: Oslo.
41. Doorman, G., et al., *Vulnerability analysis of the Nordic power system.* IEEE Transactions on Power Systems, 2006. **21**(1): p. 402-410.
42. Kjølle, G., et al., *Vulnerability of electric power networks*, in *NORDAC 2006*. 2006: Stockhom.
43. Hofmann, M., O. Gjerde, and G. Kjølle, *Vulnerability in electric power grids: State of the art and framework for vulnerability indicators*, in *SINTEF Energi. Teknisk rapport TR A7120*. 2011, SINTEF Energi: Trondheim
44. Heggset, J., G. Kjølle, and K. Sagen, *FASIT - A tool for collection, calculation and reporting of reliability data*, in *CIRED*. 2009: Prague.
45. Birkmann, J., *Measuring vulnerability to promote disaster-resilient societies: Conceptual frameworks and definitions*, in *Measuring vulnerability to natural hazards: Towards disaster resilient societies*, J. Birkmann, Editor. 2006, United Nations University Press: Hong Kong.
46. Hofmann, M., G. Kjølle, and O. Gjerde, *Development of Indicators to Monitor Vulnerabilities in Power Systems*, in *PSAM11 & ESREL 2012*. 2012: Helsinki.
47. ISO Guide, *Risk management – Vocabulary*. 2009.
48. Rausand, M., *Risk Assessment. Theory, Methods, and Applications*. Statistics in Practice. 2011, Hoboken, New Jersey: John Wiley & Sons.
49. Norges forskningsråd, *Sluttrapport SAMRISK 2006 - 2011*. 2011, Norges forskningsråd: Oslo.
50. ISO/PAS, *Societal security - Guideline for incident preparedness and operational continuity management*. 2007, ISO.
51. OED, *Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften)*, in *FOR 2012-12-07 nr 1157*. 2012, Lovdata.
52. JD, *Instruks for departementenes arbeid med samfunnssikkerhet og beredskap, Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering*, in *FOR 2012-06-15 nr 535*. 2012, Lovdata: Oslo.
53. European Energy Research Alliance (EERA) (2013) *Joint Programme on Smart Grids.* http://www.eera-set.eu/.
54. EU Commission, *GARPUR - Generally Accepted Reliability Principle with Uncertainty modelling and through probabilistic Risk assessment. Grant agreement no: 608540*. 2013, EU Commission.

55. Gjerde, O., et al., *Indicators to monitor and manage electricity distribution system vulnerability*, in *CIRED*. 2011: Frankfurt.
56. GRID, *ICT Vulnerabilities of power systems: A roadmap for future research*. 2007, The GRID consortium.
57. Gjerde, O., et al., *Risk and vulnerability analysis of power systems including extraordinary events*, in *IEEE PES Powertech* 2011: Trondheim.
58. CIGRE Working Group C4.601, *Review of the Current Status of Tools and Techniques for Risk-Based and Probabilistic Planning in Power Systems*. 2010.
59. Kjølle, G., O. Gjerde, and M. Hofmann, *Monitoring Vulnerability in Power Systems. Extraordinary Events, Analysis Framework and Development of Indicators*, in *PMAPS*. 2012: Istanbul.
60. OECD, *Guidance on safety performance indicators*, in *OECD Environment, Health and Safety Publications. Series on Chemical Accidents*. 2003: Paris.
61. Reiman, T. and E. Pietikäinen, *Indicators of safety culture – selection and utilization of leading safety performance indicators*. 2010, VTT, Technical Research Centre of Finland.
62. Kjølle, G.H., et al., *Analyser av feil og avbrudd i kraftnettet 1989 - 2011*, in *SINTEF Energi. TR A7279*. 2013: Trondheim.
63. Hofmann, M., *Vulnerability indicators for electric power grids*, in *SINTEF Energi. TR A7276*. 2013: Trondheim.
64. Union for the Coordination of Transmission of Electricity (UCTE), *Final Report - System Disturbance on 4 November 2006*. 2007.
65. Hofmann, M., et al. *Developing indicators for monitoring vulnerability of power lines - case studies*. in *CIRED - 22nd International Conference on Electricity Distribution*. 2013. Stockholm.
66. Hollnagel, E., *Barriers and accident prevention*. 2004: Ashgate Publishing Company.
67. Kjølle, G.H. and O. Gjerde, *The OPAL methodology for reliability analysis of power systems*, in *SINTEF Energi. TR A7175*. 2012, SINTEF Energi: Trondheim.
68. IEEE, *IEEE Standard Terms for Reporting and Analyzing Outage Occurrences and Outage States of Electrical Transmission Facilities. IEEE Std. 859-1987*. 1987.

Appendix

A.1 Terms and definitions

Barrier
Barrier is something that can either prevent an event from taking place or protect against its consequence [66].

Blackout
Blackout is used synonymously with wide-area interruptions resulting in severe consequences for society [The project Vulnerability and security in a changing power system].

Consequence
Consequence is outcome of an *event* [47].
There can be different types of consequences from an event:
- *economic consequences*
- *consequences on personnel/ consumers safety*
- *environmental consequences*
- *etc.*

There can be predicted more than one consequence of each type.

Contingency (outage event)
A *contingency* is an unplanned *outage* of one or more primary equipment components, i.e. one or more primary components are in the outage state [67], [68].

Coping capacity
Coping capacity describes how the operator and the system itself can cope with an unwanted event, limit negative effects, and restore the function of the system to normal state [43].

Criticality
Criticality refers to the extent of the consequences for the users of the infrastructure when a system does not carry out its intended function. The definition assumes that the concept of vulnerability also includes the consequences to society [43].

Curtailment
Curtailment is planned reduction of demand other than through market prices. Curtailment can be realized in several ways. A distinction can be made between physical curtailment by rotating disconnection or quota allocation [9].

Energy Not Supplied (ENS)
Energy Not Supplied (*ENS*) is the estimated amount of energy that would have been supplied to the end-user if the supply *fault*[5] did not occur [67].

[5] ENS is the consequence of contingencies, i.e., unplanned outages, which are due to failure events. After failure the item has a fault.

Event
Event is occurrence of a particular set of circumstances [47].

Exposure
Exposure describes if a system or parts/components are exposed to a threat and to what degree. The term exposure is used foremost in combination with natural hazards [43].

Extraordinary event
An *extraordinary event* is an event with a high societal impact and a low probability to occur.
Note: Such events are often referred to as HILP (High Impact Low Probability) events. [The project Vulnerability and security in a changing power system].

Failure, fault
A *failure* is the termination of the ability of an item to perform a required function. After failure, the item has a *fault* [IEC 60050, www.electropedia.org].

Failure is an event, as distinguished from *fault*, which is a state.

Fault is the state of an item characterized by inability to perform a required function. A fault is often the result of a failure of the item itself, but may exist without prior failure [IEC 60050, www.electropedia.org].

Interruption
An *interruption* is a condition characterized by missing or reduced supply of electric energy to one or more end users [67]. A supply interruption is a condition in which the voltage at the supply terminals is lower than 5 % of the reference voltage [Voltage characteristics of electricity supplied by public electricity networks, EN 50160:2010].

Outage
An *outage* is the state of a component or system when it is not available to properly perform its intended function due to some event[6] directly associated with that component or system [67].

Operating scenario
An *operating scenario* is 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 [adapted from [67]]. The term *operating state* is sometimes used with a similar meaning.

Power system failure
See *failure*.

Reliability of the electric power system
Reliability means the probability that an electric power system can perform a required function under given conditions for a given time interval [IEC/IEV 617-01-01]. Note: Reliability quantifies the ability of an electric power system to supply adequate electric service on a nearly continuous basis with few interruptions over an extended period of time.

Robustness
Robustness is the system's ability to withstand stress with respect to the loss of the system's function.

[6] Outages and contingencies are in this report related to *failure* events

Security of electricity supply
Security of electricity supply means the ability of an electricity system to supply final customers with electricity [4]. It can be divided into long-term and short-term security of supply. Long-term security of supply can be split into the following aspects: access to primary fuels, generation adequacy, network adequacy and market adequacy [5]. Short-term security of supply means the operational reliability (i.e., *power system security*) of the system as a whole and its assets, including the ability to overcome short-term failures of individual components of the system [5].

Susceptibility
The *susceptibility* of the infrastructure describes how likely it is that a threat leads to a disruption in the system and is depending e.g., on the technology, the working force and the organization. A system is susceptible towards a threat if it leads to an unwanted event in the system [43].

Threat
Threat can be defined as any indication, circumstance, or event with the potential to disrupt or destroy a system, or any element thereof. This definition includes all possible sources of threats, i.e. natural hazards, technical/operational, human errors, as well as intended acts such as terror and sabotage [1].

Unwanted event
An *unwanted event* can be defined as an event which can threaten the security of supply [8, 43]. The consequences of the unwanted event *power system failure* may be a *blackout* (wide-area interruption).

Vulnerability
Vulnerability is an expression for the 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 [This report, [46]]. Vulnerability is an internal characteristic of the system.

A.2 Presentations, posters, memos and media attention

The project has created a web-site presenting the project objectives and main results in terms of publications, etc.: http://www.sintef.no/Projectweb/Vulnerability-and-security/. This appendix lists the presentations, posters, memos produced in the project as well as the media attention gained during the project.

Presentations

Indikatorer som brukes i dag. Feil og avbruddsstatistikk, tidsserier 1989 – 2011
Seminar hos NVE, Oslo, 29. april 2013

Kan sårbarhet måles? Sårbarhetsindikatorer, metodikk, eksempler og case
Seminar hos NVE, Oslo, 29. april 2013

Identifikasjon av sårbarhet: Sårbarhetsanalyse av ekstraordinære hendelser
Seminar hos NVE, Oslo, 29. april 2013

"Sårbarhetsprosjektet" - Presentasjon/oversikt over hovedresultater
Seminar hos NVE, Oslo, 29. april 2013

Stormen Dagmar julen 2011 – analyser av feil og avbrudd
FASIT-dagene, Energi Norge, Gardermoen, 28. november 2012

Perceiving, Predicting & Preventing Extraordinary Events
Nettverksmøte Risikostyring Statnett 8 November 2012

Sårbarhet i kraftforsyningen. Presentasjon av prosjekt
DSB, Sandefjord, 20. Juni 2012

Fra 1992 – 2011 – Har konsekvensene av ekstremvær endret seg?
Nett- og bransjeutvikling under skiftende rammevilkår, Energi Norge, Gardermoen, 26. april 2012

Sårbarhet i kraftforsyningen og forbedringsmuligheter
SINTEF-seminar: Uten strøm også etter neste storm? Oslo, 19. april 2012

Identifikasjon av kritiske funksjoner og sårbarheter
NEKs Elsikkerhetskonferanse, Oslo, 8. – 9. November 2011

Fremtidens kraftnett, "smart grids" - smart eller sårbart?
Sikkerhetsdagene 2011, Trondheim, 10.-11. October 2011

Climate change and power systems
Workshop Risk and vulnerability in power systems in light of climate change DNV/NTNU, Trondheim, 27 September 2011

What do fault statistics tell us regarding causes resulting in power outages?
Workshop Risk and vulnerability in power systems in light of climate change DNV/NTNU,
Trondheim, 27 September 2011

Teknologisk utvikling og forsyningssikkerhet
Energiutvalget/OED, Oslo, 25. August 2011

Har vi et robust kraftsystem og hvordan måler vi det?
Nettkonferansen, Tromsø, 30. November - 1. December 2010

Sårbarhet og sikkerhet i kraftnettet
Felleskonferansen EL & IT Forbundet, NITO og Tekna, Gardermoen, 13. October 2010

A framework for analysing extraordinary events in the power system
Risk and Vulnerability in Infrastructures, Lund, 10.-11. May 2010

Forskingsformidling frå sårbarhetsprosjektet
NTNU, 2010

Energisystemets sårbarhet og muligheter knyttet til de forventede klimaendringene og behovet for tilpasning innen sektoren
NOU Klimatilpassing, Fagmøte om Energi, Oslo, 8. December 2009

Sårbarhet og forsyningssikkerhet i et kraftsystem i endring - Øker risikoen for omfattende avbrudd?
NEKs Elsikkerhetskonferanse, Oslo, 28.-29. October 2009

Sårbarhet i kraftsystemet
Seminar Samfunnssikkerhet med NVE og DSB, Trondheim, 6. October 2009

Vulnerability related to critical functions/components
RISK DSAM Workshop, Stockholm, 29. September 2009

Posters

Gerd Kjølle, Matthias Hofmann, Oddbjørn Gjerde
Monitoring vulnerability in electric power systems
The 22nd SRA-E Conference, Trondheim, 17 - 19 June 2013

Gerd Kjølle, Ruth Helene Kyte, Matz Tapper, Kenneth Hänninen:
Major storms – Main causes, consequences and crisis management
CIRED 2013, Stockholm, 10 - 13 June 2013

Matthias Hofmann, Oddbjørn Gjerde, Gerd H Kjølle, Eivind Gramme, Johan G Hernes, Jan A Foosnæs:
Developing indicators for monitoring vulnerability of power lines – case studies
CIRED 2013, Stockholm, 10 - 13 June 2013

Oddbjørn Gjerde, Gerd H Kjølle, Nina K Detlefsen, Geir Brønmo:
Risk and vulnerability analysis of power systems including extraordinary events
IEEE PES Powertech, Trondheim, 19 - 23 June 2011

Oddbjørn Gjerde, Gerd H Kjølle, Johan G Hernes, Birger Hestnes, Jan A Foosnæs:
Indicators to monitor and manage electricity distribution system vulnerability
CIRED 2011, Frankfurt, 6 - 9 June 2011

Gerd H Kjølle, Oddbjørn Gjerde, Agnes Nybø:
A framework for handling HILP events
CIRED Workshop, Lyon, 7 - 8 June 2010

Emil Johansson, Kjetil Uhlen, Agnes Nybø, Gerd H Kjølle, Oddbjørn Gjerde:
Blackout. Understanding sequence, causes and remedies of extraordinary events
IEEE PES GM, Minneapolis, 25 - 29 July 2010

Project memos

Oddbjørn Gjerde, Matthias Hofmann:
Sårbarhetsindikatorer for kraftledninger. Skagerak Nett
SINTEF Energy Research, September 2012, AN 12.12.63

Oddbjørn Gjerde, Matthias Hofmann:
Sårbarhetsindikatorer for kraftledninger. NTE Nett
SINTEF Energy Research, September 2012, AN 12.12.64

Jostein Lille-Mæhlum:
Forsyningssikkerhet i kraftsystemet – Sett i lys av Dagmar
SINTEF Energy Research, August 2012, AN 12.12.57

Silke van Dyken, Gerd H Kjølle:
State of the art regarding security of electricity supply on a European level. Policies, strategies, implementation plans and reliability standards
SINTEF Energy Research, June 2011, AN 10.12.71

Oddbjørn Gjerde:
Identification and classification of indicators. Case studies
SINTEF Energy Research, May 2011, AN 11.12.54

Agnes Nybø, Gerd H Kjølle:
Analysis of blackouts and extraordinary events in the power system
SINTEF Energy Research, March 2010, AN 09.12.46

Oddbjørn Gjerde, Randi Aardal Flo, Thomas Trötscher, Agnes Nybø:
Valg av metoder og verktøy for sårbarhetsanalyser
SINTEF Energy Research, June 2010, AN 10.12.02

Agnes Nybø, Oddbjørn Gjerde:
Scenarier for utviklingen av kraftsystemet og sårbarhet fram mot 2030
SINTEF Energy Research, June 2010, AN 10.12.64

Hanne Bakken:
Medieanalyse - sårbarhet og forsyningssikkerhet
SINTEF Energy Research, September 2010, AN 10.12.74

Hanne Bakken:
Forsyningssikkerhet og sårbarhet som tema i kraftsystemutredningar og Statnetts nettutviklingsplan
SINTEF Energy Research, September 2010, AN 10.12.75

Media attention

Performing research on vulnerability in the electric power system
(In Norwegian: Forsker på sårbarhet i kraftsystemet)
Energiteknikk no. 2, February 2010

Measuring the vulnerability
(In Norwegian: Måler sårbarheten)
Energiteknikk no. 10, December 2010

Reduces consequent failures
(In Norwegian: Minsker følgefeil)
Energiteknikk no. 7 October 2012

A.3 Methods for vulnerability assessment

This appendix lists (examples of) methods relevant for vulnerability analysis and assessment.

Vulnerability assessment	Methods
Identify critical consequences	Expert evaluation Across sector discussions Analysis of historical events Evaluation methods • Cost benefit • Risk matrix • Multi criteria decision analysis
Identify outages leading to critical consequences	FMEA/ FMECA Expert evaluation Historical events Contingency analysis – screening and ranking Simulations/contingency analysis • Power flow • Dynamic simulations • Reliability of supply • Discrete event simulations (work processes) Scenario analysis Vulnerability analysis – network theory
Identify threats that can cause the critical outages	Expert evaluation • Climate and weather information • Historical events • Fault statistics • Analysis of similar systems • Check lists HAZOP Scenario analysis
Identify vulnerabilities, susceptibility and coping capacity	Expert judgment Bow-tie model Fault tree analysis Event tree analysis Reliability block diagram
Identify factors influencing coping capacity	Expert evaluation • Climate and weather information • Historical events • Fault statistics • Analysis of similar systems • Check lists HAZOP Scenario analysis
Vulnerability evaluation, identify existing and missing barriers against critical outages	Expert judgment Bow-tie model Fault tree analysis Event tree analysis Reliability block diagram

Technology for a better society

www.sintef.no