Monitoring vulnerability in power systems

Extraordinary events, analysis framework and development of indicators

Gerd Kjølle, Oddbjørn Gjerde, Matthias Hofmann
Electric power systems
SINTEF Energy Research
Trondheim, Norway
gerd.kjolle@sintef.no

Abstract—**This paper addresses the needs for monitoring vulnerability in power systems related to extraordinary events. An analysis framework is described to identify threats, vulnerabilities, unwanted events and consequences. Vulnerability is an internal characteristic of the system comprising susceptibility and coping capacity towards natural hazards, human or technical/operational threats. Together with the external aspects of vulnerability, threats and consequences for society, vulnerability gives insight into risk related to extraordinary events. Based on this framework indicators are developed for monitoring vulnerability. For this purpose it is necessary to identify critical assets, locations and operating states. These are factors with potentials for severe consequences. Examples of vulnerability indicators are given for two different cases. The first case considers the power supply consisting of two power lines to a small community, where the main threats are storm and loading degree of the lines. The second case deals with a region where the main threat is a strained power situation due to limited generation and import capacity to the area.**

Keywords- Vulnerability; risk; indicators; extraordinary events

I. INTRODUCTION

The power system is expected to undergo major changes in coming years due to transition to smarter grids, changing power flows and increasing shares of distributed generation. Low levels of investments over many years have led to increasing utilization of the system and in many areas more strained operation. It is an ageing infrastructure and the need for reinvestments is rapidly increasing. At the same time climatic changes may impose increased stress on the grids. In this environment it is of great importance to study how vulnerability and risk related to extraordinary events and wide-area interruptions evolves. Existing data and methodologies that can be used to analyze the impact of the new challenges on risk and vulnerability mainly deals with normal or frequent events and performance data describing the history. The best available data base for documenting the reliability of supply is presumably the fault statistics. However, these data only contain information about the current components and those that have failed. Previous studies have revealed that there is a need for new knowledge and tools for monitoring vulnerability, e.g. [1, 2]. 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 technical condition of the grid and vulnerabilities.

This paper describes an analysis framework and indicators under development for the purpose of identification and monitoring of vulnerabilities related to extraordinary events with low probability and high impact, i.e. potentially leading to wide-area interruptions with severe impact on society. This framework and methodology is established in an ongoing research project in collaboration with energy authorities and network companies. The vulnerability indicators will help finding the right solutions on a regional and national level in a changing power system to ensure a sufficient level of security of electricity supply.

II. VULNERABILITY, RISK AND EXTRAORDINARY EVENTS

This chapter defines the internal and external aspects of vulnerability and presents the analysis framework for extraordinary events.

A. Definitions

Vulnerability is an expression of the problems a system will face maintaining its function when exposed to threats, and the problems the system faces resuming its activities after the event occurred (based on e.g. [1, 3]). A system is vulnerable if it fails to carry out its intended function, the 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 [3]. The power system is susceptible towards a threat if it leads to a disruption in the system. Susceptibility depends e.g. on the technology, the working 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 grid after a disruption (unwanted event). 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 [4]. Vulnerability may affect both the probability and the consequence and is as such a component of risk. Fig. 1 shows the internal and external dimensions of vulnerability.

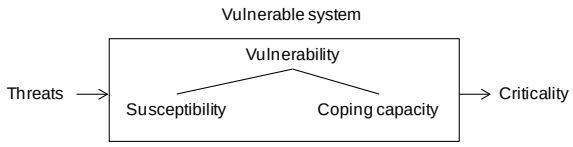

Figure 1. Internal and external dimensions of vulnerability

Threat can be defined as any indication, circumstance, or event with the potential to disrupt or destroy critical infrastructure, or any element thereof [5]. This definition may include all possible sources of threats, i.e. natural hazards (e.g. major storm), technical/operational (e.g. strained operation), human errors (e.g. digging), as well as intended acts such as terror and sabotage.

The term *criticality* in Fig. 1 refers to the level of criticality of consequences for the users of the infrastructure and not for the components in the system, assuming that the concept of risk and vulnerability also includes the consequences to society. The extent of the consequences of the unwanted event *power system failure* is for instance directly dependent on factors like how many customers are affected, what kind of customers and the duration of the interruption.

In Fig. 1 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 the coping capacity might be hampered by certain threats, like for instance traffic jam, bad weather or lack of daylight.

B. *Extraordinary Events and Analysis Framework*

The framework for vulnerability analysis is based on the bow tie-model describing the relations between main causes and consequences of an unwanted event [6, 7]. Fig. 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. This is shown in the figure together with major categories of threats.

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. As indicated in the figure, a number of barriers (B1 – B4) exist to prevent threats from developing into unwanted events and to prevent or reduce the consequences of unwanted events. In this framework a system can be defined to be vulnerable towards a threat if there is a potential for severe consequences and the existing barriers are insufficient in number or function, i.e. they

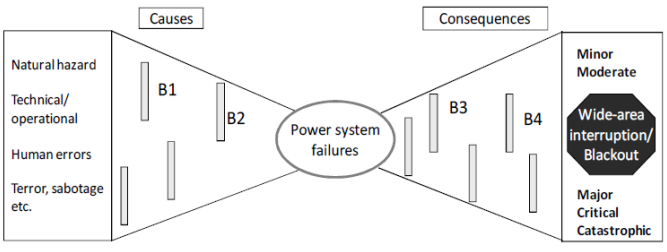

Figure 2. Threats, unwanted event, consequences and barriers

may fail to function as intended [8].

Severe consequences of interruptions will most likely be caused by combinations of power system failures since the power system (at the transmission level) is dimensioned and operated according to the N-1 criterion. Examples are a storm causing damage to several power lines, malfunction of the protection system in combination with a failure in the main grid, and failures in the distribution system resulting in loss of service in for instance transport and telecommunication. Failures combined with negatively influencing factors such as lack of situational awareness and coordination etc. might also lead to an extraordinary event [9]. Extraordinary events with high impact in terms of wide-area interruptions or blackouts usually have low probability.

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 outlined in the following chapter, based on the concept of vulnerability described above and the bow tie-model.

III. DEVELOPMENT OF VULNERABILITY INDICATORS

Indicators can be defined as observable measures that provide insights into a concept or a system that is difficult to measure directly [10]. 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*. This chapter deals with different types of indicators relevant for monitoring vulnerability in power systems. Examples are given of indicators in use today as well as possible future vulnerability indicators.

A. *Different Types of Indicators*

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 [11]:

- Outcome versus activity based indicators
- Leading versus lagging indicators.

Outcome and activity indicators monitor specific activities which are undertaken to reduce vulnerability. Outcome indicators tell you whether or not you have achieved a desired result, while activity indicators are defined as means for

measuring actions or conditions that should maintain or lead to improvements in safety [10].

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 risk and how it has been in the past
- Leading indicator: Information about how the vulnerability and risk 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 I using the technical condition of a power line as an example.

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 were collected. However, it is possible to establish a leading indicator based on these data if they are 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.

B. Indicators in Use Today

Fault statistics is probably the best available data basis for risk evaluation regarding causes of power system failures and consequences in terms of interruptions to load points. Fig. 3 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.

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 is possible to divide the faults in different classes of causes (threats). However data from the fault statistics only contain information about the current components and those that have failed, in the current system and conditions. In addition it is necessary to develop leading indicators capable of predicting the development of the vulnerability to provide information about risk exposure related to extraordinary events in a changing power system. Development of new indicators is discussed in the next section.

TABLE I. EXAMPLES OF INDICATORS RELATED TO TECHNICAL CONDITION OF POWER LINE

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

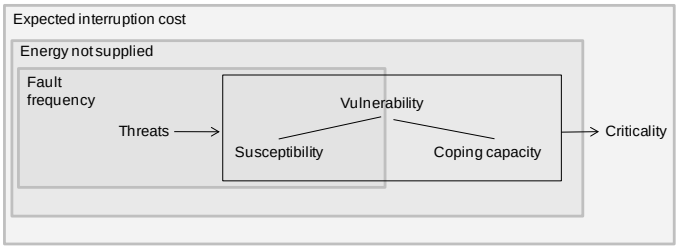

Figure 3. Examples of indicators describing parts of vulnerability

C. 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.

Vulnerability is, as explained above, related to extraordinary events. It is therefore a prerequisite for the development of vulnerability indicators to identify *critical* outages, assets, functions, locations and operating states. While the criticality dimension of vulnerability in Fig. 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 development of indicators.

Critical outages, locations etc will depend on various conditions varying among the network companies. The critical factors must be identified by each network company through a risk and vulnerability analysis using tools like preliminary hazard analysis, contingency analysis and brainstorming/ expert evaluation. Usually there is a need to combine different quantitative and qualitative methods [12].

Vulnerability indicators are supposed to cover the internal and external dimensions according to Fig. 1 and in principle there is one set of indicators for each identified threat. Based on case studies as reported in e.g. [6, 7] examples of possible indicators can be established. The framework and examples are summarized in Fig. 4.

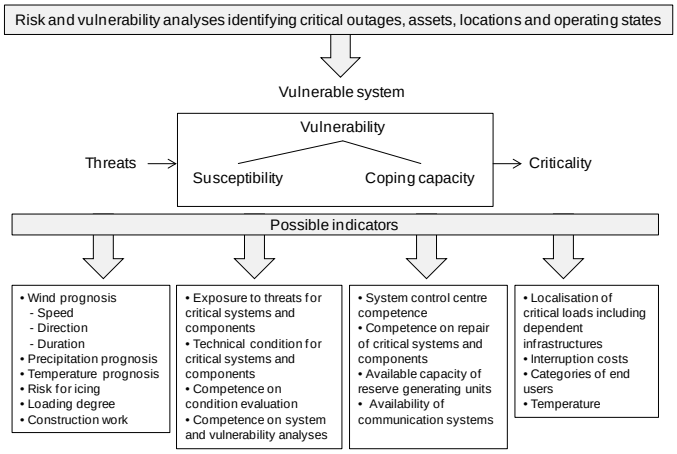

Figure 4. Framework and examples of vulnerability indicators

Fig. 4 gives examples of threat indicators for the major 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 and systems 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. Possible coping capacity indicators are related to competence on repair of critical components and systems as well as availability of 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 Fig. 4 are presented in rather general terms. For a certain network company more specific indicators are needed associated with the types of threats the network is exposed to and the related vulnerabilities. The next chapter gives examples for two different cases in Norway.

IV. Case Studies and Examples of Indicators

The first case study presented in this chapter considers the power supply to a small community located far north in Norway in a coastal area exposed to wind and icing. The second case focuses on a region in western part of Norway. The main threat for the security of supply to this region is a strained power situation due to limited generation and import capacity.

A. Case 1 – Power Supply to a Local Community

Steigen, which is a small community with less than 3000 inhabitants in Northern Norway (latitude 68°), is normally supplied by a single 66 kV overhead line while there is another line on hot stand-by. The stand-by line can be connected if the main line fails. Both lines are routed in a coastal area with harsh weather conditions, making them exposed to failures and bad conditions for repair work. In an actual event in January 2007 Steigen lost its power supply for nearly 6 days due to failures and breakdown of both 66 kV lines supplying the community. Extreme weather conditions and lack of daylight delayed repair considerably. Power supply was partially and temporarily restored using a few reserve supply units, and the available capacity in the network was shared between the different zones by rotating connections. This blackout was studied as background for the case study.

The Steigen event was triggered by heavy storm while icing was a contributing cause. This led to breakage of the line itself and damage of several pylons. The reserve line turned out not to be able to cover the load when it was connected, resulting in overheating and three subsequent line breakages. The post event fault analysis showed that these faults were caused by ageing and poor technical condition. Risk evaluations regarding power system failures and interruptions are so far typically based on the fault statistics as explained in the previous chapter. The history of faults on 66 kV lines and energy not supplied (ENS) in the supply area of the network company is shown in Fig. 5. Faults and ENS due to the event in 2007 are included in the figure.

In the ten-year period before 2007 there had been only a few faults and limited ENS on 66 kV lines in this area. Studying this period of the fault statistics gives no indication of any serious event about to happen. In a risk and vulnerability analysis however, it can be identified that overlapping faults of both lines supplying Steigen represent a critical outage since the whole community will be affected. There is no local generation in this area, and Steigen is therefore vulnerable to the loss of both lines. If such an event happens in winter the temperature might be a critical factor. In this case it can also be noted that the weather conditions as well as seasonal lack of daylight might threaten the coping capacity in terms of delayed repair and extended duration of the blackout compared to e.g. in summer time.

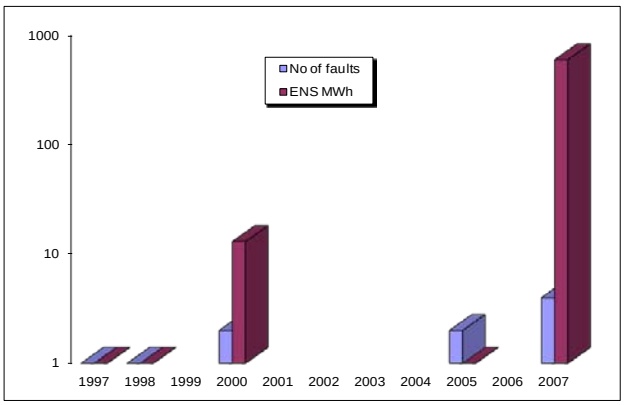

Figure 5. Local fault statistics for 66 kV overhead lines

The study has identified the following susceptibilities for the main power line:

- Slanting pylons and inadequate foundation
- Arcing damage on line due to previous faults
- Inadequate choice of right of way (holds for both lines)

For the reserve line the main susceptibility was the poor technical condition due to ageing and degradation.

Referring to Fig. 4, indicators are proposed for the threats 'storm' and 'loading degree' for this small regional network. Examples are presented in Table II.

Information about the poor technical condition of the reserve line was not possible to reveal from the fault statistics. It could only have been identified by condition monitoring and evaluation. According to the regulations on-site inspection of single components of power lines should be carried out every tenth year. For continuous monitoring and prediction of the technical condition it will thus be necessary to establish a leading indicator based on an ageing model (cf. Table I). From Table II it can be observed that the indicators for the criticality (consequences to society) are independent of the threat.

The critical assets in this case are the two 66 kV overhead lines. Appropriate susceptibility indicators are therefore the technical condition of 66 kV power lines itself as well as the competence on condition evaluation. The technical condition is an important susceptibility towards both threats 'storm' and 'loading degree'. Correspondingly, an appropriate indicator for coping capacity is the competence on repair of 66 kV lines as well as availability of spare parts and transport for repair of the overhead lines. Other indicators for the coping capacity are of a more general character (cf. Fig. 4), such as availability of communication systems and reserve generating units, although the last mentioned may depend to a high degree on the location of critical loads exposed to outages of this critical combination of power lines.

TABLE II. EXAMPLES OF INDICATORS FOR REGIONAL NETWORK

Threat	**Indicator for threat**	**Indicator for susceptibility**	**Indicator for coping capacity**	**Indicator for criticality**
Storm	Wind prognosis (speed, direction, duration)	Location in the terrain, how exposed to wind? Technical condition of 66 kV power lines Competence on condition evaluation Competence on risk and vulnerability analysis	Competence on repair of 66 kV power lines Availability of spare parts, and transport for repair of power lines Availability of communication systems and reserve generating units	Location of critical loads Types of end-users Temperature
Loading degree	Percentage loading compared to nominal values			
	Increase in loading degree			

B. Case 2 – Strained Regional Power Situation

This case study considers the power supply to a region in Western Norway (the BKK-area), where Norway's second largest city Bergen is situated. The situation is shown in Fig. 6.

The BKK-area is normally supplied from Mauranger and Fardal. Maximum load is about 1800 MW. Due to limited generation within the BKK-area there is a need for import large parts of the year. If the import need exceeds 850 MW it is not possible to fulfill the N-1 criterion. According to the transmission system operator Statnett there were more than 1700 hours in 2010 when this criterion was not met [13].

The critical event in this case is therefore 'loss of one power line if import > 850 MW'. The threat to be considered here is 'strained power situation'. Examples of indicators for this threat are given in Table III.

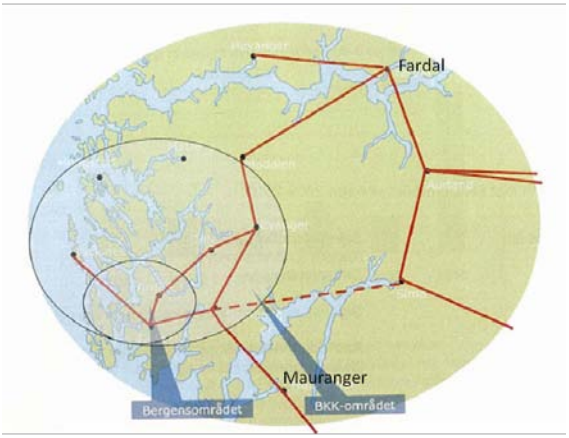

Figure 6. Power supply to Bergen and the BKK-area

TABLE III. EXAMPLES OF INDICATORS FOR THE THREAT 'STRAINED POWER SITUATION' IN THE BKK- AREA

Indicator for threat	**Indicator for susceptibility**	**Indicator for coping capacity**	**Indicator for criticality**
Fulfillment of the N-1 criterion (incl. prognosis) Import to the BKK-area, distance to import limit (850 MW) Probability of strained power situation	Technical condition of the power lines in the critical transfer corridors to BKK-area and Bergen Competence on condition evaluation of these critical power lines Competence on risk and vulnerability analysis Quality of protection schemes including system protection	Competence on restoration Access to and availability of relevant information at the control centre Availability of reserves (generation and curtailable loads) Availability of communication	Location of critical loads Types of end-users Interruption costs Temperature

Threat indicators may be the degree of fulfillment of the N-1 criterion and import need to the area, both can be identified performing contingency analysis for various operating states. The critical assets in this case are the power lines included in the critical power transfer corridors to the BKK-area and Bergen city (the inner circle in Fig. 6). Thus, the technical condition of these power lines constitutes a susceptibility indicator together with competence on condition evaluation and risk and vulnerability analysis, similarly with case 1. To increase the operational security in the BKK-area, a system integrity protection scheme (SIPS) is installed [14]. This is a load shedding scheme where some 85000 inhabitants with rather low interruption cost are automatically disconnected in case of single outages. It is of utmost importance to design the protection schemes (including SIPS) properly. The quality of protection schemes is therefore proposed as an indicator for susceptibility. Availability of relevant information and competence related to restoration as well as availability of reserves are examples of indicators for coping capacity towards the threat strained power situation.

V. Conclusions and Further Work

This paper has described an analysis framework and indicators under development for the purpose of identification and monitoring vulnerabilities related to extraordinary events with low probability and high impact, i.e. potentially leading to wide-area interruptions with severe impact on society. Vulnerability is an internal characteristic of the system comprising susceptibility and coping capacity. However, vulnerability can only be seen in relation to the external dimensions threats and the potential for severe consequences, i.e. the criticality of society. Therefore, vulnerability indicators are understood as indicators which give information about both the internal and external dimensions.

Fault statistics is probably the best available data basis today for risk evaluation regarding causes of power system failures and consequences in terms of interruptions to load points. Fault frequency, energy not supplied and expected interruption costs are examples of indicators in use based on the fault statistics. These are all lagging indicators describing past performance giving aggregate information about vulnerability. They are regarded inadequate for the purpose of monitoring threat, susceptibility, coping capacity and criticality separately. To provide information about risk exposure related to extraordinary events in a changing power system, there is a need for leading indicators capable of predicting the development of vulnerability. These vulnerability indicators will help finding the right solutions on a regional and national level in a changing power system to ensure a sufficient level of security of electricity supply.

For the purpose of developing vulnerability indicators it is not only a need to identify vulnerabilities and threats, but also the critical outages, assets, locations and operating states. These are factors with potentials for severe consequences. The critical factors can be identified through a risk and vulnerability analysis using tools like preliminary hazard analysis, contingency analysis and expert evaluation.

The framework and methodology for development of vulnerability indicators is established in an ongoing research project. Examples of vulnerability indicators are given in the paper for two different case studies with weather related and technical/operational threats. In the further work of developing indicators, it is a challenge to define appropriate leading indicators as well as scales and calculation methods for documentation of the chosen indicators. These challenges will be dealt with in collaboration with energy authorities and network companies.

References

[1] G. Doorman, K. Uhlen, G. Kjølle and E. S. Huse, “Vulnerability analysis of the Nordic power system”, IEEE Trans. on Power Systems, vol. 21, pp. 402 – 410, February 2006

[2] G. Kjølle, K. Ryen, B. Hestnes, H. O. Ween, ”Vulnerability of electric power networks”, NORDAC, Stockholm, August 2006

[3] J. Birkmann, “Measuring vulnerability to promote disaster-resilient societies: Conceptual frameworks and definitions”, in Measuring vulnerability to natural hazards, editor J. Birkmann, New York: United Nations University Press, 2006

[4] ISO/IEC guide 73: 2009 “Risk management – Vocabulary”

[5] Commission of the European communities, “Green Paper on a European Programme for Critical Infrastructure Protection”, Brussels, 2005

[6] O. Gjerde, G. Kjølle and A. Nybø, “Indicators to monitor and manage electricity distribution system vulnerability”, CIRED, Frankfurt, June 2011

[7] G. Kjølle, O. Gjerde and A. Nybø, “A framework for handling high impact low probability (HILP) events”, CIRED workshop, Lyon, June 2010

[8] A. Nybø, G. Kjølle and K. Sand, 2010, ”Vulnerability in power systems – the effect of maintenance and reinvestments”, NORDAC, Copenhagen, September 2010

[9] E. Johansson, K. Uhlen, A. Nybø, G. Kjølle, and O. Gjerde, "Extraordinary events - understanding sequence, causes and remedies," in ESREL 2010, Rhodes, September 2010

[10] OECD, “Guidance on safety performance indicators”, OECD Environment, Health and Safety Publ., Series on Chemical Accidents, Paris 2003

[11] T. Reiman and E. Pietikäinen, “Indicators of safety culture – selection and utilization of leading safety performance indicators”, VTT, Technical Research Centre of Finland, 2010

[12] O. Gjerde, G. Kjølle, N. Detlefsen and G. Brønmo, “Risk and Vulnerability Analysis of Power Systems Including Extraordinary Events”, IEEE Powertech, Torndheim, June 2011

[13] E. Hillberg, A. Holen, G. Andersson and L. Haarla, “Power System Reinforcements – the Hardanger Connection”, Paper accepted for publication in Electra, February 2012

[14] E. Hillberg, F. Trengereid, Ø. Breidablik, K. Uhlen, G. Kjølle, S. Løvlund and J. Gjerde, “System Integrity Protection Schemes – Increasing operational security and system capacity”, Paper accepted for CIGRE Session, Paris 2012