Development of Indicators to Monitor Vulnerabilities in Power Systems

Matthias Hofmann[a], Gerd H. Kjølle[a]*, Oddbjørn Gjerde[a],
[a] SINTEF Energy Research, 7465 Trondheim, Norway
*gerd.kjolle@sintef.no

Abstract: Monitoring vulnerabilities has the potential to be an essential part of power system asset management both for network companies and regulatory authorities. Vulnerability can be defined as an internal attribute of the electric power system regarding susceptibility and coping capacity towards a certain threat. Previous studies have revealed that there is a need for new knowledge on vulnerabilities in the power system including interdependencies with other infrastructures. This paper gives an overview of the state of the art in literature regarding indicators to measure the vulnerability of an infrastructure and more specifically of the power system related to extraordinary events. The needs for vulnerability indicators are identified and discussed, and a common framework and basis of essential terms for vulnerability indicators is proposed. Furthermore, a multi-step approach for developing vulnerability indicators is presented. Examples are given of possible indicators for the power system.

Keywords: Vulnerability, indicators, extraordinary events, electric power systems.

1. INTRODUCTION

Modern society is increasingly dependent on a secure electricity supply. At the same time, the electric power system is expected to undergo major changes in the coming years, raising questions such as: How do increased utilization of the network, integration of distributed generation and climate change affect the vulnerability of the ageing power system? All these aspects have an influence on the vulnerability of the power system related to extraordinary events with low probability and high impact, i.e. potentially leading to wide-area interruptions with severe impact on society. Previous studies have revealed that there is a need for new knowledge on vulnerabilities in the power system including interdependencies with other infrastructures [1, 2]. An on-going Norwegian research project seeks to provide such knowledge by looking into monitoring of vulnerabilities in the power system, thus helping to find the appropriate tools for monitoring vulnerabilities on a regional and national level. The overall goal is to achieve acceptable levels of vulnerability and reliability of electricity supply. Such monitoring of vulnerability can help to provide an adequate level of maintenance and investment and enable adequate emergency preparedness.

Due to the degree of complexity of power systems, and thus the challenge of describing vulnerability related to such systems, the use of indicators is suggested. Indicators can be defined as "observable measures that provide insights into a concept or a system that is difficult to measure directly" [3]. Indicators are useful for monitoring vulnerability, since one can create a simplified description of the power system's vulnerability and assess the expected performance and its development by combining different indicators. Such indicators are needed to describe the whole vulnerability picture in the context of extraordinary events such as wide-area interruptions.

Presently there are few indicators and data on an aggregate level to monitor and predict the vulnerabilities in power systems [1]. The best available databases for documenting this on an aggregate level are presumably fault and interruption statistics. However, these data only contain information about the current components and those that have failed. Reduced investments, less maintenance, work force reductions, and other aspects may have long-term consequences which are of vital importance for the vulnerability of the power system. Since the power system is undergoing changes that have an impact on vulnerability, there is a clear need for indicators that can give information about the future development of vulnerability, and the available indicators are found inadequate to give this information.

Other sectors, such as oil and gas, railway and nuclear power, also use indicators for measuring aspects related to risk and vulnerability (e.g. [4 - 6]). The use of indicators in these sectors is mainly aimed towards

monitoring health and safety issues, as well as risk for major accidents and thus also measuring the vulnerability as an inherent part of this risk. However, these indicators cannot be directly applied to the power system, since they are adapted to the specific needs of their sectors. Still, the theoretical framework and experiences are a valuable input to the development of vulnerability indicators for the power system.

This paper describes a framework for development of indicators capable of monitoring vulnerability in power systems. The concept of vulnerability, its dimensions and relation to risk of extraordinary events is discussed in Section 2 with the aim to develop a common basis of the most essential terms for vulnerability indicators. Section 3 looks into existing indicators that can be used as an input for the development of vulnerability indicators, whereas Section 4 establishes the indicator development process. The theoretical framework is summarised in Section 5 and illustrated with examples of vulnerability indicators for power systems in Section 6, before the conclusions are presented in Section 7.

2. THE CONCEPT OF VULNERABILITY

2.1. Defining vulnerability

A clear definition of vulnerability is essential for developing vulnerability indicators. Even though vulnerability is a well-known concept, there is no common definition. For example, Thywissen [7] lists 29 different definitions for the term vulnerability which can be found in the literature. The many definitions are due to the use of the term vulnerability in different disciplines. Often vulnerability refers to vulnerability of societies or the population and not to the vulnerability of a system or infrastructure. Even the vulnerability definitions for critical infrastructures and in particular the power system are different [8 - 14].

Depending on the various definitions the system is exposed to unwanted events, threats or hazards of which the source can be outside or both outside and inside of the system. The consequences are also defined differently. A system's vulnerability is threat specific and closely connected to the system's ability to maintain its function when exposed to threats. Consequences can be restricted to the immediate consequences which are the loss of function. Other definitions also include the ability to restore normal function or even widen the perspective of vulnerability by including the consequences for the users of the infrastructure. In addition, several factors (physical, social, economic, and environmental) that have an influence on the vulnerability of a system can be considered.

Although different definitions exist, a core concept of vulnerability can be found; vulnerability describes how a system faces problems to carry out its intended function when exposed to materialised threats/hazards/events. The following definition of vulnerability is used as the basis in this paper for the development of vulnerability indicators for power systems:

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. 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. Vulnerability is an internal characteristic of the system.

2.2. Dimensions of vulnerability

The vulnerability of critical infrastructures can be divided into several dimensions to form a general framework for analysing vulnerability [15, 16]:

- Threat / hazard and unwanted event
- Exposure
- Susceptibility
- Coping capacity
- Criticality.

Based on these dimensions and the chosen definition of vulnerability, a general vulnerability framework can be outlined as shown in Figure 1. While vulnerability is regarded as an internal characteristic of the system itself, threats and criticality are external dimensions.

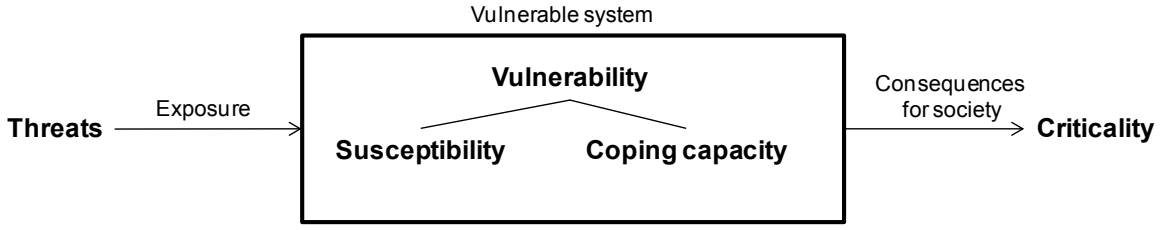

Figure 1. General vulnerability framework

Threats and *hazards* are defined in different ways in the literature [9, 11, 12, 17, 18]. The term threat often includes hazards or can be used interchangeably with hazards. Based on [11], the term threat can be defined as follows providing an all-hazard approach: *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. Threats are evolving outside of the system.*

Threats can be categorized into nature/weather related threats, human threats and operational conditions/threats. A threat may lead to an unwanted event, understood as a disruption of the system such as power system failures, leading to interruptions of electricity supply. Examples of threats in different categories are for example given in [17, 19 - [21].

In the general framework in Fig. 1 the vulnerability of the system is divided into *susceptibility* and *coping capacity*. The susceptibility of the infrastructure describes if a threat leads to a disruption in the system and is depending on for instance the technical components, the working force and the organization. On the system level other factors like institutional and social factors also have influence on the susceptibility. Based on various literature sources (e.g. [13, 15, 16, 22]) the following definitions of susceptibility and coping capacity are extracted: *A system is susceptible towards a threat if the threat leads to an unwanted event in the system. The coping capacity describes the ability of the operator and the system itself to cope with an unwanted event, limit negative effects, and restore the function of the system to normal state.*

Several aspects are influencing the susceptibility and coping capacity (e.g. [15, 16, 23, 24]). Table 1 summarises technical, human related (working force), and organizational aspects.

Table 1. Examples of internal system aspects with influence on the susceptibility and coping capacity

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

The criticality of an infrastructure can best be measured by the dependency of the society on that infrastructure [15, 19]. The term criticality is here used for the consequences for the users of the infrastructure. *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 severity of the consequences can be measured by several factors such as affected population/area, duration of the interruption, economic consequences, societal consequences, and consequences for health and life (see e.g. [11, 19, 24, 25]).

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

2.3. Risk and vulnerability

The goal of the work presented in this paper is to develop indicators for monitoring vulnerability related to extraordinary events in power systems. Extraordinary events can be defined as events with low probability and high impact. For this purpose we need to identify unwanted events, their likelihood and potential impact, which is mainly described by the risk of such events. Risk and vulnerability are closely connected and there is consent that vulnerability is a component of risk even though risk can be defined in many ways (see e.g. [11, 12, 15, 17, 18, 26 - 29]). A common definition of risk is based on the ISO Guide 73:2009. According to this standard, risk is a combination of the consequence of an event, and its associated likelihood. As vulnerability describes the susceptibility towards threats and the coping capacity related to unwanted events, vulnerabilities may affect both the probability and the consequence and is as such a component of risk.

3. INDICATORS IN USE TODAY

Indicators are already widely used in power system asset management, for different purposes and with different degree of detail, quality and awareness. Examples are indicators based on fault and interruption statistics as used in Norway, distinguishing between fault frequency, energy not supplied and costs of energy not supplied [30]. The different dimensions covered by these indicators are illustrated in Figure 2. 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. it includes the duration of the interruption and therefore also the time to restore the grid functionality. Cost of energy not supplied (CENS) additionally covers the criticality of the interruptions by the number and types of customers who were affected and their consequences. These three indicators are aggregated in the sense that they cover more than one dimension of the vulnerability framework and are as such inadequate for the purpose of monitoring the various dimensions of vulnerability.

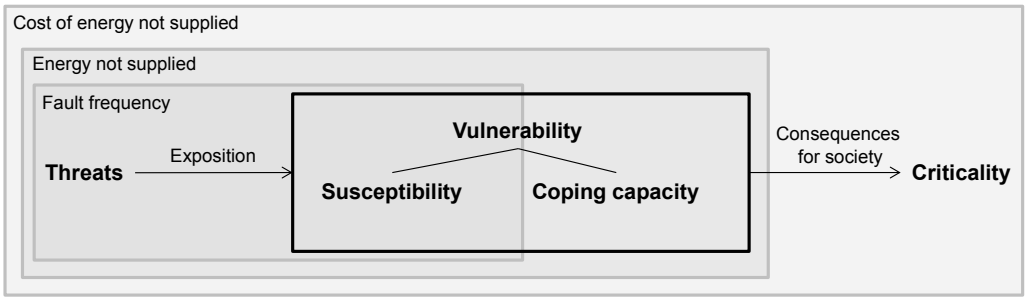

Figure 2. Vulnerability dimensions covered by fault frequency, energy not supplied and cost of energy not supplied

Other examples are the indicators defined by the Swedish Energy Agency to monitor reliability of supply in Sweden [31], where the scope of these indicators is to cover energy and capacity shortage. However, most of these indicators do not focus on the vulnerability of the power system, but rather on *reliability of supply* aspects. These indicators can therefore only be used in addition to other indicators with a focus on vulnerability, as the vulnerability indicators should be capable of monitoring changes in the different dimensions of the vulnerability (as given in Figure 1). These findings state that new vulnerability indicators have to be developed.

4. INDICATOR DEVELOPMENT

4.1. Types of indicators

There exist a wide range of categorizations of indicators (see e.g. [3, 32, 33]). Safety indicators are the main focus in the literature, but it is assumed that the categories used for safety indicators are applicable also for vulnerability indicators. The categories regarded appropriate to give a complete picture of vulnerability are *leading* and *lagging*, as well as *activity* and *outcome* indicators. The distinction between leading and lagging indicators depends on which system and type of events that are studied and the methods and perspectives (organizational, technical etc.) used. In general, leading indicators provide information about the foreseen development and can, if properly designed, be useful as predictors, while lagging indicators provide

information about performance in the past. Regarding power system vulnerability, fault frequency, ENS and CENS based on fault statistics are typical examples of lagging indicators, while a leading indicator could for instance be based on a model predicting the technical condition of the components. Outcome and activity based indicators are closely connected to specific actions. Activity indicators can be understood as means for measuring actions or conditions that should maintain or lead to improvements in vulnerability, whereas outcome indicators are designed to measure whether such actions are, in fact, leading to the expected improvements [3]. Therefore outcome indicators can tell you whether or not you have achieved a desired result. Activity indicators are usually easy to measure since they are connected to activities, while the outcome indicators have to be observed over a longer period of time. In addition, outcome indicators are often a result of many factors making it challenging to extract the effect of a given activity. The indicator categories can be summarized as:

- *Lagging indicator: Information about the current vulnerability and how it has been in the past.*
- *Leading indicator: Information about how the vulnerability of the system will develop in the future.*
- *Activity indicator: Information about the level of targeted activities to reduce vulnerability.*
- *Outcome indicator: Information about if the targeted activity has led to a reduction in vulnerability.*

4.2. Development process

Various approaches for the development of indicators are applied in different sectors (e.g. [5, 6, 34 - 36]). Based on these approaches, the process for developing vulnerability indicators can be summarised by several steps, as presented in Figure 3.

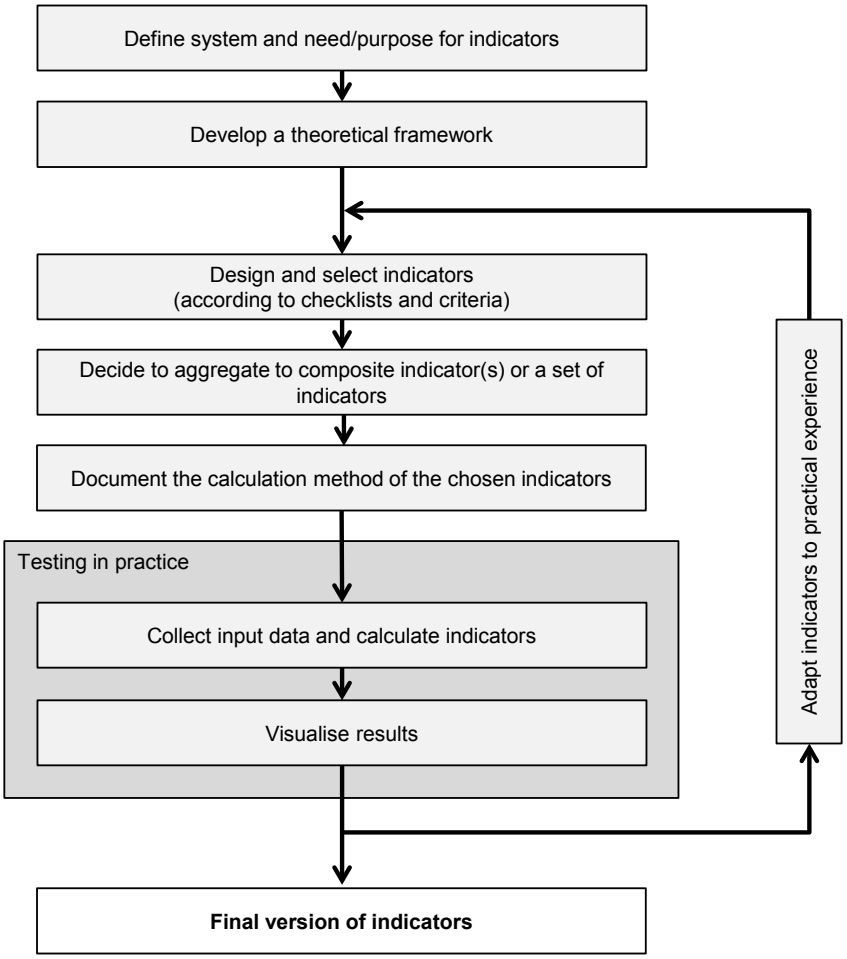

Figure 3. Process for developing vulnerability indicators

The first step of indicator development is to define the scope of the indicators. A common understanding can be reached by defining the system of interest and identifying the purpose of and the need for indicators. In the second step, a theoretical framework has to be developed where all the aspects with influence on vulnerability should be defined together with a nested structure of sub-aspects of vulnerability. Based on this

structure it should be clarified what types of indicators are needed to describe the different aspects of vulnerability.

The third step is to design suitable indicators to cover the relevant aspects of vulnerability for the given purpose. This step also includes the definition of scales and the provision of appropriate calculation methods to report the chosen indicators in a consistent manner. It can be suitable to describe each indicator according to a standardized template. If the number of indicators is large or if the goal is to summarise the multi-dimensional aspects of vulnerability, it can be necessary to aggregate indicators into a composite indicator or a set of indicators. The use of composite indicators is always a trade-off between giving a simplified, but easier to understand picture of the vulnerability situation, and a detailed picture which may be necessary to really understand the underlying causes for changes in vulnerability.

After the selection of indicators these have to be tested in practical cases to get feedback from the prospective users of the indicators. As a consequence, data have to be gathered to establish the indicators, e.g. through available data and statistical sources. If the data needed are not available, actions need to be defined to get hold of it, for example through surveys. A visualisation of the results helps the user to capture trends and other relations more easily. The design, calculation methods, scales, aggregating rules, and the visualisation of the indicators should further be adapted according to the experience from the practical testing. This loop of improving and testing the indicators should be performed until a final version of indicators is reached.

4.3. Indicator quality

The quality of the indicators should be evaluated during the development process. The evaluation can partly be based on the feedback from the testing phase, but should also be based on a given set of criteria and a checklist. The quality evaluation serves two purposes. First, checklists support the search for good indicators and help to check if an indicator is adequate for the aspect the indicator shall represent. Secondly, it helps to improve the quality of the indicator by using the checklist as an active support tool in the review of the indicator. Different criteria exist for the evaluation of an indicator and several checklists can be found in the literature (e.g. [24, 37, 38]). Based on these sources, the following checklist is developed:

- Is the indicator relevant for the purpose of monitoring vulnerability?
- Does the indicator monitor a relevant aspect?
- Is the indicator as simple as possible while still serving the purpose?
- Are underlying assumptions and limitations identified?
- Is the indicator ‘measurable’ / quantifiable?
- Is it possible to obtain the required data for calculating the indicator?
- Does the indicator have the required accuracy?
- Is the indicator related to a quantified target value or is at least the direction of positive trend defined?
- Is the indicator clearly defined and is it clearly stated how it is calculated?
- Is the indicator suitable for communicating vulnerability?
- Is it trusted and accepted by involved stakeholders?

5. FRAMEWORK FOR POWER SYSTEM VULNERABILITY INDICATORS

A framework for the vulnerability indicators in power systems is developed based on the presented state of the art [39]. The indicators should address all dimensions (threats, susceptibility, coping capacity, and criticality) regarding the vulnerability of the power system and subsequent aspects to give a complete picture of the vulnerability. A distinction between the indicator types leading/lagging and activity/outcome indicators is regarded as suitable for monitoring vulnerability. The operators of the power system have limited influence on the threats and the criticality of the consequences for society, as these are external dimensions. Consequently, they can only influence on the susceptibility and coping capacity. Therefore, activities will usually be related to the vulnerable system and not the external environment. Thus, activity and outcome indicators are only meaningful for monitoring susceptibility and coping capacity. Figure 4 illustrates the general framework for vulnerability indicators and related indicators for threats and criticality based on the state of the art [39]. This framework comprising all the different dimensions and the types of

indicators helps to keep an overview if all important aspects of vulnerability are covered with adequate indicators and helps to structure the process of finding and developing indicators.

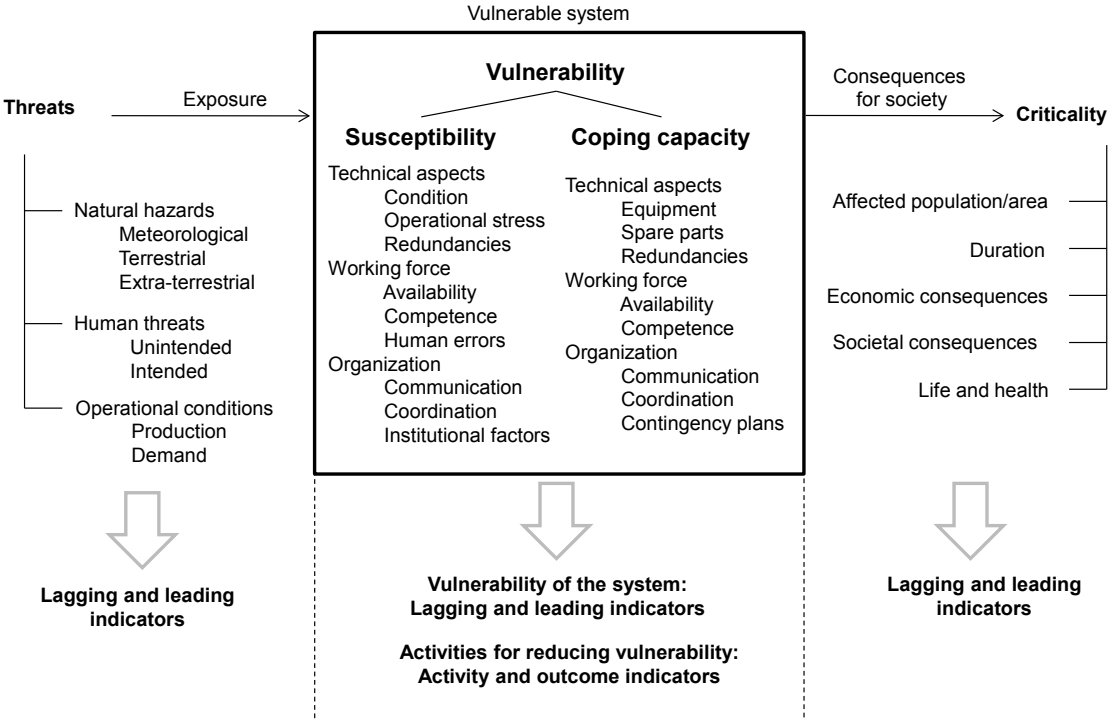

Figure 4. Theoretical framework for vulnerability indicators for the power system [39]

6. INDICATOR EXAMPLES

Construction of vulnerability indicators must be preceded by a risk and vulnerability analysis, identifying critical outages, assets, locations, and operating states in the power system. Tools for such analyses can be preliminary hazard analysis, contingency analysis and brainstorming or expert judgement, see e.g. [40]. As a part of these analyses each stakeholder should define the term "critical". In this way the vulnerabilities are identified, making it possible to identify vulnerability indicators within the relevant dimensions. Examples of possible vulnerability indicators for a network company are presented in Table 2 for three different threats (storm, digging and overload of system and components) within the major categories natural hazard, human threat and operational conditions.

The following can be observed based on the work with indicator examples as shown in Table 2:

- In principle there are one set of indicators for each identified threat.
- Indicators for susceptibility depend to a high degree on the specific threat.
- Indicators for coping capacity and criticality are to a large extent independent of the specific threat, except when it comes to competence (and spare parts etc.) on specific components needing e.g. repair.
- Coping capacity might be hampered by certain threats, like for instance weather conditions, traffic problems or unavailability of communication systems.

As the coping capacity will be appropriate for several threats and unwanted events, it also seems likely that an indicator for coping capacity will provide relevant information on vulnerability against threats that are not earlier identified. In general, indicators for coping capacity and criticality tend to cover more aspects in terms of different types of unwanted events, and thus might be more all-embracing compared to indicators for threats and susceptibility. The indicators in Table 2 are presented in rather general terms. For a given network company more specific indicators are needed associated with the types of threats the network is exposed to and the related vulnerabilities.

Table 2. Examples of different threats and possible corresponding indicators for monitoring vulnerability

	Indicator for threats	**Indicator for susceptibility**
Natural hazard: Storm	Wind prognosis Historical wind data	Localisation (exposure to wind) of critical power lines Technical condition of critical power lines Competence on condition evaluation of power lines Competence on system analyses and vulnerability evaluations
Human threat: Digging	Construction work near critical locations in the power system Historical data on cable joint failures	Number and localisation of junctions where infrastructures meet Technical condition of power cables including joints Competence on condition evaluation of power cables including joints Competence on system analyses and cross sector vulnerability evaluations
Operational conditions: Overload	Overload Stepwise increase in loading degree	Loading degree for critical systems and components Technical condition of critical systems and components Competence on condition evaluation of critical components Competence on system analyses and vulnerability evaluations

	Indicator for coping capacity	**Indicator for criticality**
All threats	System control centre competence (including cooperation and coordination between infrastructures) Competence on repair (of power lines, cables, other critical components) Available transport for repair (of power lines, cables, other critical components)	Localisation of critical loads including dependent infrastructures Interruption costs including dependent infrastructures Categories of end users affected Temperature

7. CONCLUSION

The paper gives an overview of the state of the art in literature regarding indicators to measure the vulnerability of an infrastructure and more specifically of the power system. The needs for vulnerability indicators are identified and discussed, and a common basis of essential terms for vulnerability indicators is established. Furthermore, a framework for vulnerability indicators is proposed and a multi-step approach for developing indicators is presented. Examples of possible indicators for power systems are given.

The main contribution of this paper is the establishment of a foundation for development of vulnerability indicators. Important aspects for understanding the vulnerability are outlined and discussed including threats, aspects which influence the susceptibility and coping capacity of the infrastructure, and also criteria for measuring the consequences to society. Based on this framework, it must be decided for which aspects vulnerability indicators should be developed. First of all, only vulnerabilities which have the potential to lead to major impact on society should be included, meaning a blackout or wide-area interruption. Even though blackouts have a low probability of occurrence, they do happen. Blackouts are often caused by a combination of different circumstances or events, such as coinciding failures in the main grid, failures in

combination with malfunction of protection or planned outages, inadequate system operator response, or adverse weather causing wide-area damage on power lines. Secondly, it is important to give attention to vulnerabilities related to increasing climatic stress, ageing infrastructures and a strained power balance which leads to a higher utilization of the grid.

Further work will be to create indicators for selected vulnerabilities, to be used in vulnerability management and for power system planning and operation purposes.. Furthermore, the indicators have to be tested with the two main user groups; the grid operators and the authorities/regulators. Network companies can use the indicators in their daily operations and for power system planning, whereas authorities/regulators need indicators for their overall supervision of grid operators and for the development of regulatory aspects.

Acknowledgements

This work is part of the research project "Vulnerability and security in a changing power system" funded by the Norwegian Research Council, Norwegian energy authorities and network companies.

References

[1] Kjølle, G. H., Ryen K., Hestnes B., Ween H. O.: Vulnerability of electric power networks. Nordic Electricity Distribution and Asset Management Conference (NORDAC), Stockholm (Sweden), 2006.
[2] Doorman, G., Uhlen, K., Kjølle, G. H., Huse, E.: Vulnerability Analysis of the Nordic Power System. IEEE Transactions on Power Systems, 21(1), 402–10, 2006.
[3] OECD: OECD Guidance on safety performance indicators - Guidance for Industry. Public Authorities and Communities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response, 2003.
[4] Øien, K., Utne, I. B., Herrera I.: Building Safety indicators: Part 1 – Theoretical foundation. Safety Science ,49(2), 148–61, 2011.
[5] Oljedirektoratet: Utvikling i risikonivå norsk sokkel: Pilotprosjektrapport 2000. Oljedirektoratet, Oslo 2001. (In Norwegian)
[6] Vinnem, J. E.: Risk indicators for major hazards on offshore installations. Safety Science, 48(6), 770–87, 2010.
[7] Thywissen, K.: Core terminology of disaster reduction. In: Birkmann, J., editor. Measuring vulnerability to natural hazards: Towards disaster resilient societies, United Nations University Press, Hong Kong 2006.
[8] NOU. Når sikkerheten er viktigst: Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner. NOU 2006:6, Oslo 2006. (In Norwegian)
[9] Holmgren, Å. J.: Quantitative Vulnerability Analysis of Electric Power Networks. Doctoral Thesis. Royal institute of Technology, Stockholm 2006.
[10] DEMA. DEMA's Approach to Risk and Vulnerability Analysis for Civil Contingency Planning. Internet document. http://www.brs.dk/folder/nationalsaarbarhedsrapport2005/Background_paper_ on_ DEMAs_approach_to_risk_and_vulnerability, Accessed 2011-04-08
[11] Commission of the European Communities. Green paper on a European programme for critical infrastructure protection. Commission of the European Communities, Brussel 2005.
[12] President's Commission on Critical Infrastructure Protection. Critical foundations - Protecting America's infrastructures. The Report of the President's Commission on Critical Infrastructure Protection, 1997.
[13] United Nations International Strategy for Disaster reduction (UN/ISDR): Living with Risk: A global review of disaster reduction initiatives. United Nations publications, Geneva 2004.
[14] Kröger, W., Zio, E.: Vulnerable Systems. Springer, London 2011
[15] Lenz, S.: Vulnerabilität kritischer Infrastrukturen. Forschung im Bevölkerungsschutz 4, Bonn 2009. (in German)
[16] Birkmann, J., Bach, C., Guhl, S., Witting, M., Welle, T., Schmude, M.: State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom/Stromausfall. Forschungsforum Öffentliche Sicherheit 2010. (in German)
[17] American Lifelines Alliance: Guideline for Assessing the Performance of Electric Power Systems in Natural Hazard and Human Threat Events. Federal Emergency Management Agency (FEMA), National Institute of Building Sciences (NIBS), 2005.

[18] Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP): Threat analysis - Threats to Canada's Critical Infrastructure. 2003.
[19] International Risk Governance Council (IRGC): White paper on managing and reducing social vulnerabilities from coupled critical infrastructures. Geneva 2006.
[20] DEMA. National Sårbarhedsudredning. Sekretariatet for National Sårbarhedsudredning, Birkerød 2004. (In Danish)
[21] Bittner, R., Günther, K., Merz, B: Naturkatastrophen in Deutschland. Hochwasserschutz und Katastrophenmanagement, 6, 7–10, 2009. (In German)
[22] Johansson, J.: Risk and Vulnerability Analysis of Interdependent Technical Infrastructures: Addressing Socio-Technical Systems. Doctoral Thesis. Lund University, Lund 2010.
[23] International Risk Governance Council (IRGC): Managing and reducing social vulnerabilities from coupled critical infrastructures: Policy brief. Geneva 2007.
[24] Kjølle, G. H.: Sårbarhetsindikatorer (og indikatorer for forsyningssikkerhet). SINTEF memo 08.12.50, Trondheim 2009. (In Norwegian)
[25] Doorman, G., Kjølle, G. H., Uhlen, K., Huse, E. S., Flatabø, N: Vulnerability of the Nordic Power System. SINTEF report, TR A5962, Trondheim 2005.
[26] United Nations International Strategy for Disaster reduction (UN/ISDR): Living with Risk: A Global Review of Disaster Reduction Initiatives. United Nations publications, Geneva 2002.
[27] North American Electric Reliability Corporation (NERC): Reliability Considerations from the Integration of Smart Grid. Princeton 2010.
[28] Birkmann, J.: Measuring vulnerability to promote disaster-resilient societies: Conceptual frameworks and definitions. In: Birkmann J., editor. Measuring vulnerability to natural hazards: Towards disaster resilient societies, United Nations University Press, Hong Kong 2006.
[29] Aven, T.: On how to define, understand and describe risk. Reliability Engineering & System Safety , 95 (6), 623–31, 2010.
[30] Heggset, J., Kjølle, G. H., Sagen, K.: FASIT – A tool for collection, calculation and reporting of reliability data. CIRED 2009, Prague 2009.
[31] Statens Energimyndighet (Swedish Energy Agency): Indikatorer för försörjningstrygghet. ER 2007:04. Eksilstuna 2007. (In Swedish)
[32] Reiman, T., Pietikäinen, E.: Indicators of safety culture – selection and utilization of leading safety performance indicators. Swedish Radiation Safety Authority. Report number 2010:07, 2010.
[33] Hopkins, A.: Thinking About Process Safety Indicators. Safety Science, 47 (4), 460–5, 2009.
[34] Øien, K.: Remote Operation in Environmentally Sensitive Areas; Development of Early Warning Indicators. Proceedings 2nd iNTeg-Risk Conference, Stuttgart (Germany) 2010.
[35] Nardo, M., Saisana, M., Saltelli, A., Tarrantola, S., Hoffman, A., Giovannini, E.: Handbook on constructing composite indicators: Methodology and user guide. OECD Statistics Working Paper, Paris 2005.
[36] Hiete, M., Merz, M.: An Indicator Framework to Assess the Vulnerability of Industrial Sectors against Indirect Disaster Losses. International ISCRAM Conference, Gothenburg (Sweden) 2009.
[37] Statens Energimyndighet (Swedish Energy Agency): Guide till indikatorjungeln - Indikatorer inom energiområdet. ER 1:2002, Eksilstuna 2002. (in Swedish)
[38] Sand, K.: Risk indicators for distribution system asset management. SINTEF report, TR A6787, Trondheim 2009.
[39] Hofmann, M., Gjerde, O., Kjølle, G. H.: Vulnerability in electric power grids: State of the art and framework for vulnerability indicators. SINTEF report, TR A7120, Trondheim 2011.
[40] Gjerde, O., Kjølle, G. H., Detlefsen, N. K., Brønmo, G.: Risk and vulnerability analysis of power systems including extraordinary events. IEEE PowerTech, Trondheim (Norway) 2011.