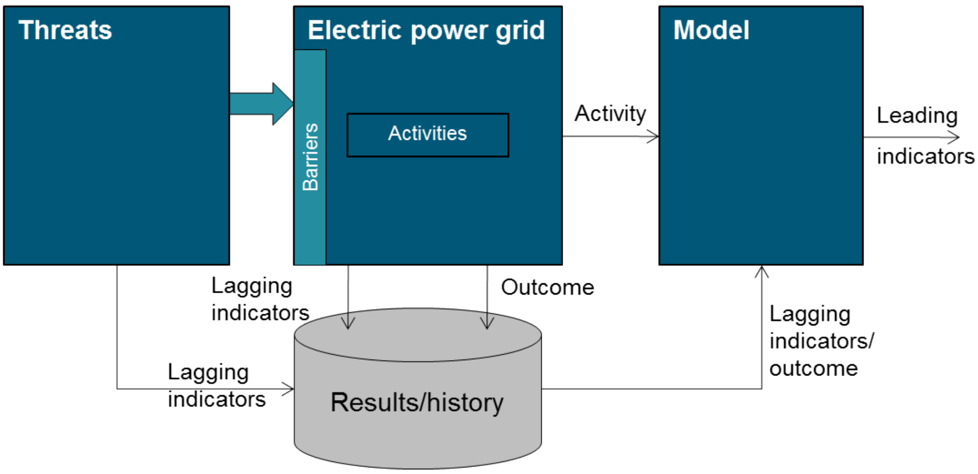
TR A7276- Unrestricted

Report

Vulnerability indicators for electric power grids

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



SINTEF Energy Research
Electric Power Systems
2013-07-25

SINTEF

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

Report

Vulnerability indicators for electric power grids

KEYWORDS:
Vulnerability
Security of supply
Power systems
Indicators

VERSION
1.0

DATE
2013-07-25

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

CLIENT(S)
Research Council of Norway, multiple clients

CLIENT'S REF.
Erland Staal Eggen

PROJECT NO.
12X618

NUMBER OF PAGES/APPENDICES:
34

ABSTRACT

This report presents a framework and methodology to develop indicators to monitor the vulnerability of the electric power grid. It establishes a scientific foundation by defining vulnerability and the different dimensions threat, susceptibility, coping capacity and criticality. The process of indicator development is described and exemplified with cases studies from two grid operators and selected critical power lines in their supply area. Several example indicators are developed with focus was on the technical condition of the power lines. The theoretical framework and the practical experiences with the case studies showed that the development of leading indicators which can give information about the future vulnerability is still a remaining research challenge.

PREPARED BY
Matthias Hofmann

SIGNATURE

CHECKED BY
Maria Daniela Catrinu-Renström

SIGNATURE

APPROVED BY
Knut Samdal

SIGNATURE

REPORT NO.	ISBN	CLASSIFICATION	CLASSIFICATION THIS PAGE
TR A7276	978-82-594-3538-5	Unrestricted	Unrestricted

Table of contents

1 Introduction ... 5

2 Purpose and scope of indicator development ... 6

2.1 Purpose ... 6

2.2 Scope of indicator development ... 7

2.3 System boundaries ... 7

3 Framework for development of vulnerability indicators ... 8

3.1 Definition of vulnerability ... 8

3.2 Types of indicators ... 9

3.3 Dimensions of vulnerability ... 10

3.4 Identification of critical outages, assets, functions, locations and operating states ... 13

3.5 Process and methodology for vulnerability indicator development ... 13

3.6 Checklists and evaluation criteria ... 15

4 Examples of vulnerability indicators and influencing factors ... 16

4.1 Vulnerability indicators ... 16

4.2 Vulnerability influencing factors ... 17

5 Case studies ... 19

5.1 Selection of indicators ... 19

5.2 Data sources ... 20

5.3 Assignment of indicator values ... 20

5.4 Aggregation and weighting ... 22

5.5 Indicator results ... 24

5.6 Indicator quality ... 26

5.7 Methods for designing leading indicators ... 27

6 Discussion ... 30

7 Conclusions and further work ... 31

8 References ... 32

1 Introduction

The report is a delivery from the project "Vulnerability and security in a changing power system", work package 1 (WP1) "Indicators and framework for monitoring of vulnerabilities". The goals of this work package have been to:
Address the need for indicators and methodical framework that can be used to measure, monitor and classify vulnerabilities, and thereby, enhance the understanding of vulnerabilities in electric power grids, e.g. related to the degree of utilization, degree of backup supply, extreme weather, societal costs of interruptions etc.

This work has resulted in proposed vulnerability indicators and a methodological framework for vulnerability and security assessment. The vulnerability indicators and framework will serve a range of purposes for different stakeholders (energy authorities, system operators and network companies), such as:

- Risk and vulnerability analysis of transmission and distribution systems.
- 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 of network companies.
- Decision making in planning and operation of the changing power system.
- Contingency and emergency preparedness planning.

The aim of this report is to establish a scientific foundation for the development of indicators and to test some indicators in real life case studies. In detail, it describes the indicator development process with examples and presents the application of some indicators based on case studies with grid operators.

2 Purpose and scope of indicator development

This chapter gives the theoretical background for the indicator development by clarifying the general scope of the project and confining the electric power grid as it is used in these report.

2.1 Purpose

The state of the art report for vulnerability indicators gives the theoretical basis for the indicator development [1]. It showed that different concepts for vulnerability are in use and that vulnerability can be specified by different dimensions. Based on these concepts a general framework for vulnerability has been extracted. This framework uses the dualistic approach of vulnerability with susceptibility and coping capacity. In addition, it gives a comprehensive insight into the whole risk picture by including threats and the consequences for society. These four dimensions form the general vulnerability framework as applied in the development of vulnerability indicators.

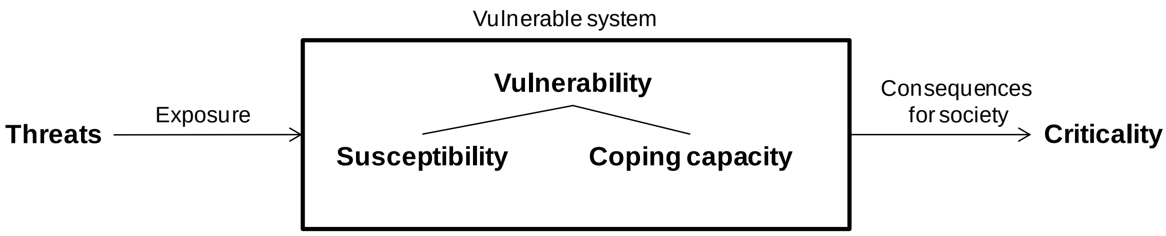


Figure 2-1 General vulnerability framework.

The state of the art report summarized also the use of indicators for measuring aspects related to risk and vulnerability in other sectors, such as oil and gas, railway and nuclear power. The use of indicators in these sectors aims mainly towards monitoring health and safety issues, as well as risk for major accidents and thus, measuring the vulnerability as an inherent part of this risk. However, these indicators cannot be transferred directly 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 report shows how the general vulnerability framework can be adapted to the electric power grid based on the concepts presented in the state of the art report. It also applies the indicator development with some example indicators used in several case studies.

2.2 Scope of indicator development

Presently there are few indicators and data available on an aggregate level to monitor and predict the vulnerabilities in power systems [2]. The best available database for documenting this on an aggregate level is 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. A clear need for indicators that can give information about the future development of vulnerability is identified, since the power system is undergoing changes that have an impact on vulnerability. The available indicators are found inadequate to give this information.

Based on the scientific state of the art, the indicator development is focused on selected aspects of vulnerability. First of all, only vulnerabilities are included which have the potential to lead to a major impact on society, which means a blackout or wide-area interruption. 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, planned outages or inadequate system operator response, or adverse weather causing wide-area damage on power lines. Second, a main focus should lie on vulnerabilities associated with increased climatic stress, ageing infrastructure and a strained power balance which leads to a higher utilization of the grid.

2.3 System boundaries

The general vulnerability framework distinguishes between the vulnerable system, here the electric power grid, and the external threats and users of that infrastructure. The system boundaries of the electric power grid as used in this report are defined in such a way that it is possible to distinguish between the vulnerable system and the surroundings. The correct definition of system boundaries will allow for the identification of a concise set of indicators that covers the most important aspects of vulnerability. All aspects that can be influenced directly by the grid operator are defined as part of the vulnerable system whereas all other factors that influence vulnerability are outside the system boundaries. The operators of the electric power grid have limited control on the threats and the criticality of the consequences for society and these dimensions are therefore external dimensions.

However, at different system levels the vulnerable system can change depending on the definition of the electric power grid on these levels. In this report, the focus is on the electric power grid that is controlled by a grid operator/company. On the company level, the main focus is on the needs of the grid operators. Here, the system consists of the electrical infrastructure (for example, electric power lines and sub stations), the resources the operator has, as the working force and technical equipment, and the organization of the company. The indicators presented in this report focuses on the company level. Other factors influencing vulnerability at this level are controlled by authorities and are defined as external factors. The authorities control many grid operators and their interactions through the regulatory framework. However, regardless of the control level, the function of the electrical infrastructure is to provide secure electricity supply to the customers and the society in general.

3 Framework for development of vulnerability indicators

This chapter presents the theoretical framework used for the development of vulnerability indicators as proposed [1] and [3].

3.1 Definition of vulnerability

A clear definition of vulnerability and a description of a framework that covers all dimensions of vulnerability are needed before one can develop vulnerability indicators. Although different definitions exist in literature, a core concept of vulnerability can be found [4]. Based on this concept and the definition of "Sårbarhetsutvalget" (NOU 2000:24) the following definition of vulnerability is used as the basis for the development of vulnerability indicators:
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.

The definition of vulnerability describes several dimensions that together form a complete picture of vulnerability. These dimensions are:

- threat
- 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 2-1. While vulnerability is regarded as an internal characteristic of the system itself, threats and criticality are external dimensions.

The vulnerable system is an infrastructure that is exposed to threats at different levels. Threats can be understood as an all-hazard approach and are 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* [5].

To determine if a system is vulnerable to a threat, one must consider the dualistic concept of susceptibility and the coping capacity of the system. In general, 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. *The power system is susceptible towards a threat if it leads to an unwanted event in the system. 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 an unwanted event.* Susceptibility depends e.g., on the technology, the working force and the organization. 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. Vulnerability may affect both the probability and the consequence and is as such a component of risk.

The consequences of an unwanted event having negative effects on society can best be measured by the dependency of the user on that infrastructure. The term criticality describes the consequences for the users and is defined as: *the extent of the consequences for the users of the infrastructure when a system does not carry out its intended function.*

All definitions presented in this chapter are further elaborated in [1] where details and different definitions are compiled.

3.2 Types of indicators

The general vulnerability framework presented in the previous section must be adapted to describe the vulnerability aspects of the electric power grid that should be measured with indicators. According to [6] indicators can be defined as *"observable measures that provide insights into a concept or a system that is difficult to measure directly"*. The indicators should address all dimensions (threats, susceptibility, coping capacity, and criticality) of the vulnerability of the electric power grid and subsequent aspects to give a complete picture of the vulnerability. There are different types of suitable for monitoring vulnerability in the electric power grid:

- 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.

Table 3-1 gives some examples for the different indicator types. The technical condition of a power line and its development in future is a good example for lagging and leading indicators. 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 3-1 Examples of different types of vulnerability indicators [1].

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

The operators of the electric power grid have limited influence on the threats and the criticality of the consequences for society, as these are external dimensions. Consequently, they can only influence susceptibility and coping capacity of the electric power grid. Therefore, activities will usually be related to the vulnerable system and not the external environment, and activity and outcome indicators are only meaningful for monitoring susceptibility and coping capacity.

The different types of indicators are in relation to each other. Activities will change the future vulnerability and have therefore a direct influence on leading indicators that measure the vulnerability. In addition, the future vulnerability is dependent on the current level of vulnerability (measured with lagging indicators) and the effectiveness of the activities (measured with outcome indicators of comparable activities and historical data). To create leading indicators, all this information must be processed in a model for prediction of vulnerability. These interdependencies of the different indicator types are illustrated in Figure 2.

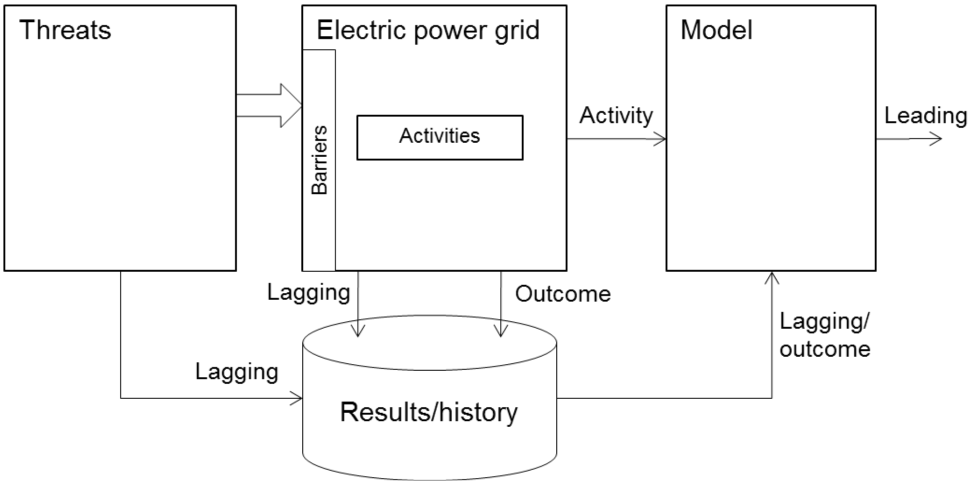


Figure 3-1 Relations between different indicator types.

For the purpose of the project it was found most relevant to focus on lagging and leading indicators. These indicators can cover all dimensions of the vulnerability.

3.3 Dimensions of vulnerability

Figure 3-2 illustrates the framework for the assessment of vulnerability indicators for the electric power grid and related indicators for threats and criticality. This framework comprises all the different dimensions and the types of indicators and helps to give an overview of all important aspects of vulnerability in the electric power grid that might be covered by adequate indicators. In addition, it helps to structure the process of selecting and designing indicators.

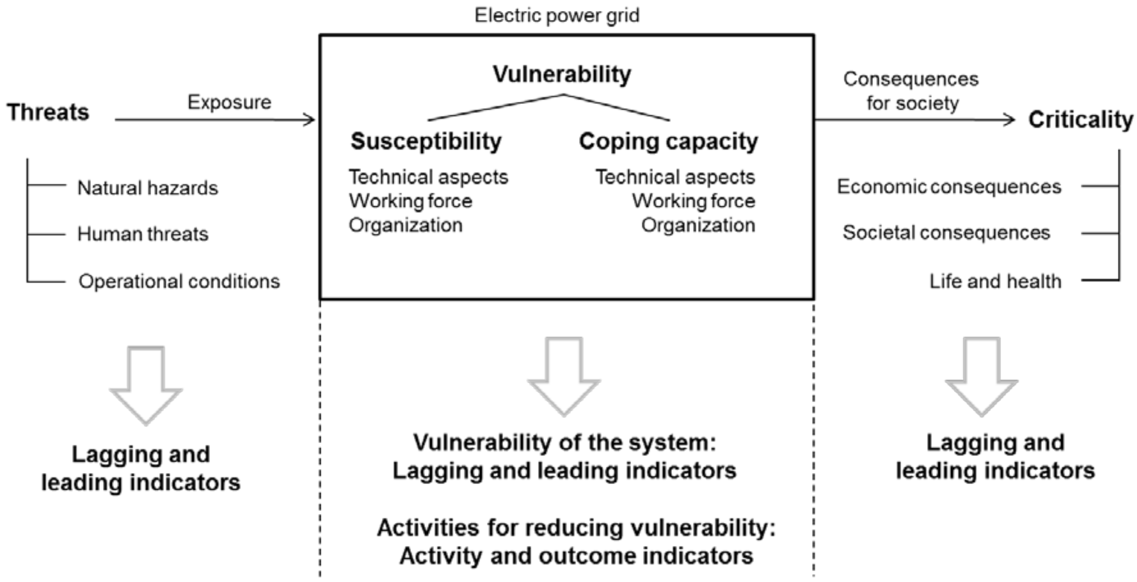


Figure 3-2 Vulnerability framework for the electric power grid [1], [3].

Threats against the electric power grid are an external dimension of vulnerability that can be categorized into natural hazards, human threats and operational conditions. It is meaningful to distinguish between natural hazards and human actions as sources of threats. In addition, the operational conditions that are influenced by the electricity generation and demand should be considered. Natural hazards can again be classified based on the source of the hazard; meteorological (weather related), terrestrial (for example vegetation, animals etc.), and extra-terrestrial (mainly solar storms). Human actions are divided into intended and unintended actions to distinguish between events like accidents and terrorist attacks. Furthermore, it is of advantage to have the information if a threat has the potential to affect a local or regional area to describe the possible geographical extent of exposure for the electric power grid. Table 3-2 summarizes the different threats and their sub categories.

Table 3-2 Categorization and examples of threats for the electric power grid, based on [1].

		Examples	Possible area affected
Natural hazards	Meteorological	Storms (wind, snow, ice, salt, etc.)	Regional
		Flood	Regional
		Lightning	Local
		Extreme temperature	Regional
	Terrestrial	Avalanches, land slides	Local
		Vegetation	Local
		Animals	Local
		Non-pandemic and pandemic disease	Local/regional
	Extra-terrestrial	Solar storms	Regional
Human threats	Unintended action	Construction activity	Local
		Accident (car, plane, etc.)	Local
	Intended action	Sabotage	Local/regional
		Terrorism (physical, cyber)	Local/regional
		Cyber attacks	Local/regional
Operational conditions		Generation	Local/regional
		Demand	Local/regional

The analysis of vulnerability of the electric power grid can be based on the analysis of different components and parts of the system. The electric power grid's vulnerability to a certain threat depends on the susceptibility and the coping capacity. The internal characteristics of the system that have an influence on the susceptibility and the coping capacity can be categorized in the three categories: technical aspects, working force and organization. That means that repair equipment, communication systems, human resources and the organization are considered in addition to the technical infrastructure.

The susceptibility of the electric power grid describes if a threat leads to a disruption in the system and depends on for instance the technical condition of components in the system, availability of personnel and operative competence. On the system level other factors have also an influence on the susceptibility. These can be for example the capacity of the network and its utilization, privatization and liberalisation, and the complexity of the organization structure for the whole power system with owners, operators, regulators, etc.

The coping capacity describes how the operator and the system itself can cope with the situation and restore the function of the grid when a failure in the grid has occurred. It can be discussed if factors as redundancies and the (N-1)-criterion should be treated as part of the susceptibility or as part of the coping capacity. This question is closely related to the definition of what is understood as an unwanted event. A single failure in the electric grid could be defined as an unwanted event even if no direct consequences for the function of the grid occur. Then, redundancies would be part of the coping capacity since they would be used to reduce the consequences after the unwanted event has occurred. However, if the unwanted event is defined as an interruption of the power supply, redundancies would be part of the susceptibility since they could be used to prevent the unwanted event. Redundancies and the (N-1)-criterion are in this report regarded as part of the susceptibility while the coping capacity is foremost seen in relation to the preparedness of the organization. The emergency preparedness also includes the three dimensions technical, human and organizational. The technical equipment, spare parts and the human resources must be available to be able to repair the failures occurring in the system. The organization for emergency preparedness with contingency and communication plans should be in place. Table 3-3 summarises the most important aspects of susceptibility and coping capacity related to the electric power grid.

Table 3-3 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 ▪ Transport
Human related (working force)	▪ Availability of personnel ▪ Operative competence ▪ Human errors	▪ Availability of personnel ▪ Competence 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

The criticality of consequences for society if a power interruption occurs can be different based on the dependency of these users on electricity ([7], [8]). The extent of the consequences is directly dependent on factors such as, how many customers are affected, what kind of customers and the duration of the interruption. In addition, factors like the geographical area affected, outdoor temperature and the potential disturbance of other societal critical functions may have an influence on the consequences [9]. The disconnected load and the amount of energy not supplied give an indication of the consequences for society and should be related to the users affected. The following aspects should be for example analysed in order to determine the criticality of the consequences for society (see e.g. [5], [8], [10], [11] [9]):

- affected population/area
- duration of the interruption
- economic consequences
- societal consequences
- health and life

In Norway factors affecting the different vulnerability dimensions are predominantly: storms (threat), technical condition of power lines (susceptibility), situational awareness (coping capacity), repair competence (coping capacity) and consequences for society if other critical infrastructure is affected (criticality).

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

Storms causing wide area interruptions by damaging critical power lines are a major threat in Norway [12], [13]. Such storms affect large areas causing falling trees and often salt contamination of electrical equipment and can lead to long lasting power interruptions. Technical condition is an important factor for the susceptibility of power lines as shown by the event in Steigen in 2007 [14]. If an unwanted event (power system failure) have led to interruption in the power supply, it is important to be aware of the situation and to have the right competence available to allow for a fast restoration of the power supply. Both factors are crucial for the coping capacity of a grid operator as often shown in the analysis of historical events [15]. Consequences of unwanted events in the electric power grid are especially critical if other infrastructures and societal functions are affected. One example is the fire in a cable culvert in Oslo S induced by a cable damage that also led to damages of the communication infrastructure and to disruptions in the public train transport [9], [16].

3.4 Identification of critical outages, assets, functions, locations and operating states

After having defined vulnerability more in detail and the different dimensions of vulnerability, the next step is to find suitable indicators that cover the relevant aspects of vulnerability according to the analysis framework presented above. Vulnerability is, as explained earlier, related to extraordinary events in this project. 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 Figure 3-2 refers to the consequences for the end-users and 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 [17].

3.5 Process and methodology for vulnerability indicator development

As discussed in [1] other sectors use indicators mainly for monitoring health and safety issues, as well as risk for major accidents and thus, they measure the vulnerability as an inherent part of the risk. These indicators cannot be transferred directly to the power system, but the theoretical framework applied for the development of vulnerability indicators can be used. Different approaches for the development of indicators are applied in these sectors (e.g. [18], [19], [20], [21]). Based on these approaches the process for developing vulnerability indicators can be summarised by several steps, as presented in Figure 3-3.

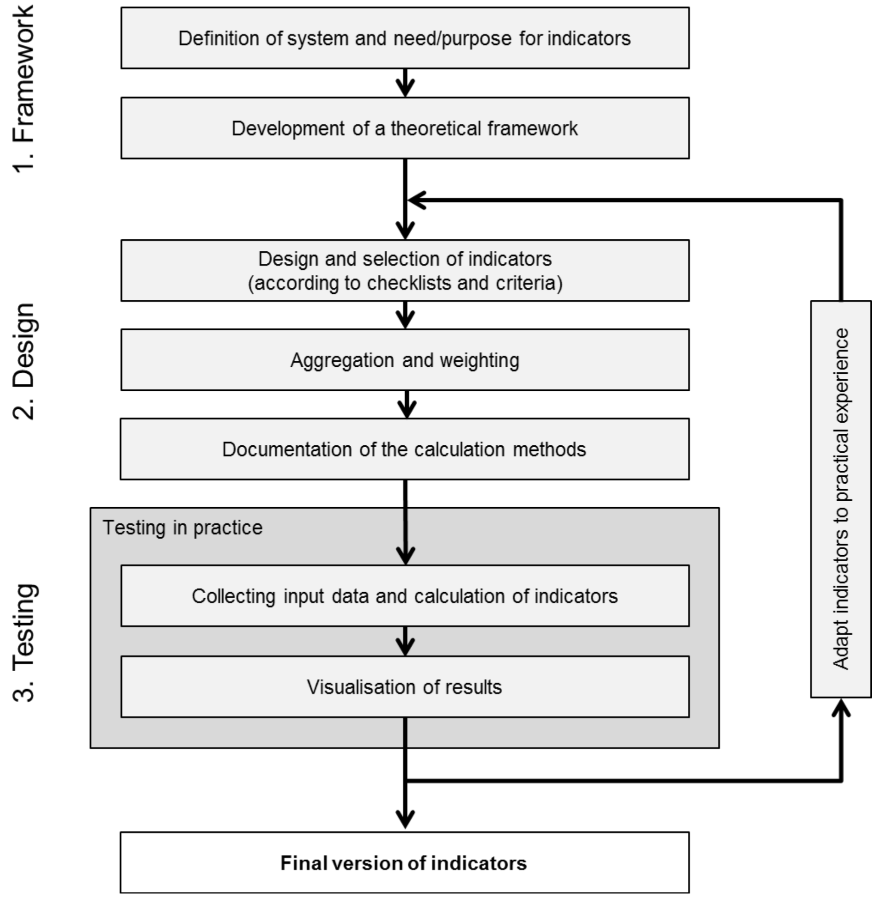


Figure 3-3 Indicator development process, based on [3].

The first step of indicator development is to define the scope of the indicators. Therefore, it should be clarified how the system of interest is confined to surroundings to ensure a common understanding of the system the indicators shall be applied to. In addition, the purpose of the indicators needs to be identified and what expectations and needs the different users of the indicators have. In this project, the users of the indicators are the network operators and energy authorities. For these users, a theoretical framework has been developed where all the aspects with influence on vulnerability of the electric power grid are defined together with a nested structure of sub-aspects of vulnerability. This structure helps to visualise what types of indicators are needed to cover the different aspects of vulnerability. This step of the indicator development is described in the previous sections of this chapter which presents the vulnerability framework applied in this project.

The second step comprises the actions to be taken for designing suitable indicators that can satisfy the needs formulated in the first step and that cover the relevant aspects of vulnerability for the given purpose. First of all, observations should be selected that can be measured by indicators and give information about the vulnerability aspects one is interested in. After the selection, it should be decided how indicators should be designed and calculated to give useful information that can be interpreted in an easy way. This process includes also the definition of scales so that the indicator can be compared to other indicators and eventually can be aggregated to a higher level. Parts of this work should be performed by stakeholders and experts of the electric power grid, preferably during workshops where different aspects can be discussed directly in group interaction to reach a mutual agreement on the basic properties of the indicators. It also needs to be decided if indicators should be aggregated to a higher level or if several indicators should be combined into one indicator. 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. All indicators and calculation methods as well as data sources used should be documented in a transparent way. The different methods available for this step of the indicator development are explained more in detail and exemplified with case studies for the electric power grid in chapter 5.

In the third step, the designed set of indicators should be tested in practical cases to see if the data are available in the expected quality and to get feedback from the possible users of the indicators. As a consequence, data must be gathered to establish the indicators, e.g., through available data and statistical sources. If the data needed is not available, additional effort must be done in order to obtain it, for example through surveys. After the calculation of the indicators, the results should be presented in an easy readable form, preferably as figures or graphs to help the user to capture trends and other relations more easily. All the experience obtained at this step should be used to refine or change indicators until a final set of indicators is available that fulfils the expectations of the users and the goals as specified in the first step.

3.6 Checklists and evaluation criteria

Checklists and criteria should be developed for the evaluation of proposed indicators 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. [10], [22], [23]).

A checklist and evaluation criteria should focus on the following aspects:

- Relevance (meaning) for the user
  - Is the indicator relevant for the purpose of monitoring vulnerability?
  - Is the indicator suitable for communicating vulnerability (and risk)?
  - Is the indicator as simple as possible while still serving the purpose?
  - Is the indicator related to a quantified target value or is at least the direction of positive trend development defined?
- Availability
  - Is the indicator ‘measurable’ / quantifiable?
  - Is it possible to obtain the required data for calculating the indicator?
  - Does the data/indicator have the required accuracy?
- Reliability
  - Are data regarded as being objective and without significant sources of error?
  - Are underlying assumptions and limitations identified?
  - Is the indicator clearly defined and is it clearly stated how it is calculated?
- Completeness
  - Is the final set of indicators complete, i.e. monitoring all major types of threats, susceptibility, coping capacity and criticality for the influencing factors chosen?
- Ownership
  - Is it trusted and accepted by involved stakeholders?

4 Examples of vulnerability indicators and influencing factors

Different indicators can be useful for monitoring the vulnerability of the electric power grid and there are various vulnerability influencing factors related to technical and organizational aspects, as well as the work force. This chapter gives examples of vulnerability indicators and influencing factors.

4.1 Vulnerability indicators

Table 4-1 gives examples of threat indicators for the major categories natural hazard, human threats and operational conditions and sets them into relation to indicators for susceptibility and coping capacity. A susceptibility of the electric power grid is always direct dependent on a given threat. On the other hand coping capacity covers several threats since it will allow for a restoration of the power grid regardless the reason and therefore the threat that lead to the unwanted event. However, in some cases specific competence/repair equipment is needed for specific components of the electric power grid as for example sea cables.

Table 4-1 Examples of different threats and possible corresponding indicators for monitoring vulnerability.

	Indicator for threats	Indicator for susceptibility
Natural hazard: Storm	▪ Wind prognosis (speed, direction, duration) ▪ Historical wind data	▪ Localization (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
Natural hazard: Icing	▪ Precipitation prognosis ▪ Temperature prognosis ▪ Historical precipitation and temperature data	▪ Localization 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 locations 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

	Indicator for coping capacity	Indicator for criticality
All threats	▪ System control center 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) ▪ Available capacity of reserve generating units ▪ Availability of communication systems	▪ Localization of critical loads including dependent infrastructures ▪ Interruption costs including dependent infrastructures ▪ Categories of end users affected ▪ Temperature

Weather prognosis of wind, snow and icing parameters will be relevant indicators for weather related threats for instance in Norway. The existence of other external factors such as construction activities (outside the electrical system) or digging works in an area can be 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.

The indicators in the table are presented in rather general terms. Possible coping capacity indicators are related to the available competence to repair 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 in the table. The table 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.

4.2 Vulnerability influencing factors

Each network company has to develop specific indicators that will be associated with the specific types of threats the network is exposed to and the related vulnerabilities. The indicators should be relevant to describe the specific factors that influence company's vulnerability and clear rules must be identified of how the indicators should be measured.

A workshop has been organized within the project to discuss vulnerability aspects of the Norwegian power system. The workshop gathered grid operators and authorities that identified factors and indicators of interest to understand and measure the vulnerability. The workshop focused on the internal dimensions of vulnerability (susceptibility and coping capacity) without taking into account the threat perspective (as described in chapter 4.1.). In these dimensions, the most important factors in the groups of technical aspects, working force and organization were found and proposals for the type of indicator (lagging, leading or activity) were given. The identified indicators with corresponding measurable units are presented in Table 4-2.

Table 4-2 Examples of factors of susceptibility and coping capacity important for the Norwegian power grid.

		Factors	Indicator description	Indicator type
Susceptibility	Technical aspects	Loading degree	Loading degree of components in the electric power grid.	Lagging
		Loading degree	Monitoring power transfer corridors and distance to thermal limit.	Lagging
		Technical condition	Technical condition and condition development of components in the system. Executed maintenance. Estimation of future condition based on operation scenarios.	Leading
		Criteria for dimensioning	Changes in dimensioning criteria over time and number of components that are dimensioned based on "old" criteria.	Lagging
		Condition monitoring	Number of inspections of physical equipment.	Activity
	Working force	Formal competence	Formal competence of the working force (skilled workers, engineers etc.) in relation to the need for competence.	Lagging
		Competence demand	Balance between retirement of working force and access to new graduated persons.	Lagging
	Organization	Regulatory framework	Income regulations and if they allow to invest in a robust grid and a stable economic situation in the companies.	Lagging
		Process time for investments	Time elapsed from the planning phase until the investment decision is made and commissioned, including the licensing process for new investments in the electrical power grid.	Lagging
Coping capacity	Technical aspects	System protection	Increasing/decreasing use of system protection (load tripping schemes, generation tripping schemes and network separation).	Lagging
	Working force	Competence test	Number of exercises and real failure situations.	Activity
		Formal competence	Formal competence of the working force (for example, skilled workers, engineers etc.) in relation to the need for competence.	Lagging
		Competence demand	Balance between retirement of working force and access to new graduated persons.	Lagging
	Organi-zation	Reserve transformers	Cooperation agreements between grid operators to share spare parts.	Activity

5 Case studies

Several indicators were developed in two case studies that were performed together with grid operators to test whether the theoretical framework can be applied to real cases. This chapter summarizes the steps of indicator development in these case studies. In addition, the experiences gained through the case studies are summarised.

5.1 Selection of indicators

It is almost impossible to cover all aspects of vulnerability in the electric power grid. Therefore, the challenge is to decide on relevant aspects that should be focused on and what indicators can give information that describes those aspects in a satisfactory manner. It is important to avoid details and aspects that may have no significant influence on vulnerability.

The focus of the indicator development in the case studies has been on lagging indicators and especially on the condition of selected power lines for two reasons. First of all, the technical condition is identified as an important factor with influence on the vulnerability and secondly, grid operators have data available from their maintenance system that can be used to construct indicators. The indicators are based on the locations of the electricity poles. The technical condition of the power line relates to all dimensions of vulnerability. It was chosen to establish indicators for all four dimensions of vulnerability as illustrated in Figure 5-1.

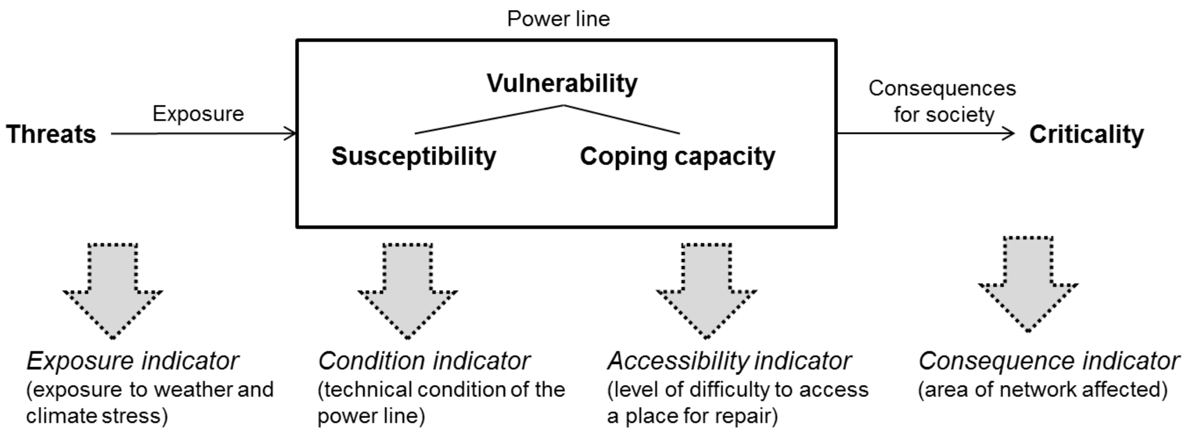


Figure 5-1 Selected vulnerability indicators for the case study of power lines.

The indicator for threat focuses on weather and climate stresses that either can cause an immediate failure or can lead to deterioration in the technical condition of the power line. Susceptibility is covered by an indicator that presents the technical condition of the power line based on data from periodically conducted maintenance inspections. Coping capacity is described by an indicator that looks into the accessibility of the pole location for repair work if a failure occurs. This is estimated based on the time needed to reach that location and gives therefore an estimate for time to restoration. Consequences for society are measured with an indicator that is based on the location of critical loads and power switches in the network since they give an indication for the number of end users affected.

5.2 Data sources

Data that is used for the calculation can be found in different sources. A main question is whether data needed for an indicator development is already available or if data have to be collected for that purpose. Regardless the data source, timeliness and quality of data are of great importance for the calculation of all indicators. While the quality of data is often dependent on a subjective evaluation, it is relatively easy to determine the timeliness of the data based on the collection date. It is important to investigate how fast data can change to get to a relevant statement for timeliness. Five year old data may be up to date in some cases, while they may be outdated in others. Some data, as for example historical data of weather and climate conditions can only change significantly in decades and it is therefore applicable even though it has not been updated for several years. Other information such as the technical condition of components can change more rapidly. Especially at the end of the forecasted life time, condition may be reduced at higher speeds. Therefore, this information should be updated regularly to assure the timeliness. Other information as for example geographical data or technical data regarding the network in general has only to be updated if major changes are apparent.

In the case study, the assignment of values to the indicators is based on different data sources. The indicator for technical condition is based on data from maintenance inspections where information about deviations in accordance to a checklist is collected. This data is usually updated during different inspections that are performed regularly, i.e. each year, each 5th or 10th year. All other indicators were based on available information material as maps and reports. Table 5-1 summarizes the different data sources for the indicators.

5.3 Assignment of indicator values

In general, the indicators can be obtained with three different approaches:

- expert assessments (subjective)
- calculations based on data (objective)
- mixture of subjective and objective approach

Expert assessments can be obtained by asking experts and their knowledge directly how they would evaluate an indicator based on a given scale. The answers would present the subjective opinion of the experts and therefore the approach is completely dependent on finding the right experts with knowledge needed for assigning a value to an indicator of interest.

The other approach calculates the indicator based on the available data and can therefore be considered as a more objective approach. This approach is more demanding since it is dependent on several factors. First of all, one has to decide what data should be used to calculate the indicator. Second, a calculation rule has to be established and the scale of the indicator has to be defined. It is also important that the indicator value is explained and set in context so that the indicator value can be understood. It is always favourable to use similar scales for all indicators, since it should be easier for the user to interpret the indicators in a larger context and in comparison to other indicators.

A mixture of the aforementioned approaches is also possible meaning that experts would give their opinion based on data or models. All approaches can be used for lagging as well as leading indicators. However, in general, indicator values based on data are preferable since they can be verified and the underlying assumptions that lead to the indicator are transparent.

In the case studies, the assignment of values to the indicators is based both on expert assessments and on calculations. Only the indicator for technical condition is calculated based on data from maintenance inspections where information about deviations is collected in accordance to a checklist. All checklist points with no relation to vulnerability as for example missing information plates are ignored for this calculation. Each deviation is rated with a condition reduction based on the severity of the deviation. The data contain three different levels of severity and therefore it is decided to relate the severity levels to a condition reduction of 25, 50 and 75. These values are subtracted from 100 that represent perfect condition. The deviation values are summed if several deviations for one electricity pole location occur. Consequently, it is possible that condition values can drop below zero. In this case they are rounded to zero. The condition indicator can therefore take only values of 0, 25, 50 or 100.

All the other indicators (exposure, accessibility, consequence) are quantified based on a subjective assessment of the available information. The assessment leads to an indicator value in five categories, which are ranged from, for example, extreme to low exposure to climate. The exposure indicator is based on information given directly from the network companies and reports about corrosion, ice loads and wind speeds at different locations in the grid. Accessibility of the different pole locations and therefore the time to reach them in case of repair are estimated with map material and the specification of the infrastructure available (for example path, road, field) for these locations. Long distance to roads and locations at islands and in the mountains are assigned worse indicator values than locations close to roads. Consequences for society of power interruptions at different locations in the analyzed power line are based on the location of circuit breakers and the location of critical loads together with a subjective assessment of the possible consequences.

All indicators use the same qualitative scale from 0 to 100 where 0 is the worst value and 100 the best value. It is decided to use the same scale for all indicators mainly to allow for comparison of different indicators and a more straight forward aggregation of indicators. Table 5-1 summarizes the main properties of the developed indicators.

Table 5-1 Indicators chosen and methods for value assignment.

Indicator	Data source	Method	Scale
Exposure indicator	Reports about corrosion, wind speed and ice loads at different locations	Expert assessment based on available data	0 – extremely exposed 100 – little exposed (in steps of 20)
Condition indicator	Reported deviations by inspection, from the maintenance system	Calculation based on data	0 – very poor condition 100 – no deviation from perfect condition (in steps of 25)
Accessibility indicator	Map material	Expert assessment based on available data	0 – very difficult accessibility 100 – easy accessibility (in steps of 20)
Consequence indicator	Location of circuit breakers and location of critical loads	Expert assessment based on available data	0 – critical consequences 100 – marginal consequences (in steps of 20)

5.4 Aggregation and weighting

All indicator values are estimated per electricity pole location to find special vulnerable points in the network. Once the indicators are determined, it should be decided if and how the indicators can be aggregated. In general, several factors can lead to the need to aggregate indicators. If the number of indicators is large or if the goal is to summarise the multi-dimensional aspects of vulnerability into one or a few indicators, it can be necessary to aggregate indicators into a composite indicator or a smaller set of indicators. The use of aggregation 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.

In general, two different aggregation approaches and the combination of these approaches are available when aggregating indicators. The first approach is to aggregate the same indicators from a lower to a higher system level. This can be, for example, the aggregation of a vulnerability indicator from different grid operators to one indicator for a larger region that is covered of these companies. Such an indicator will still have the same scale and content, but will give information for a larger region and not only for the single companies. The second approach is to aggregate different indicators to a combined indicator that includes information of all these indicators. An example is the aggregation of several indicators that cover different aspects of the susceptibility into one indicator that gives an overview of the susceptibility situation. Both approaches can also be used together as illustrated in Figure 5-2 and applied in the case studies.

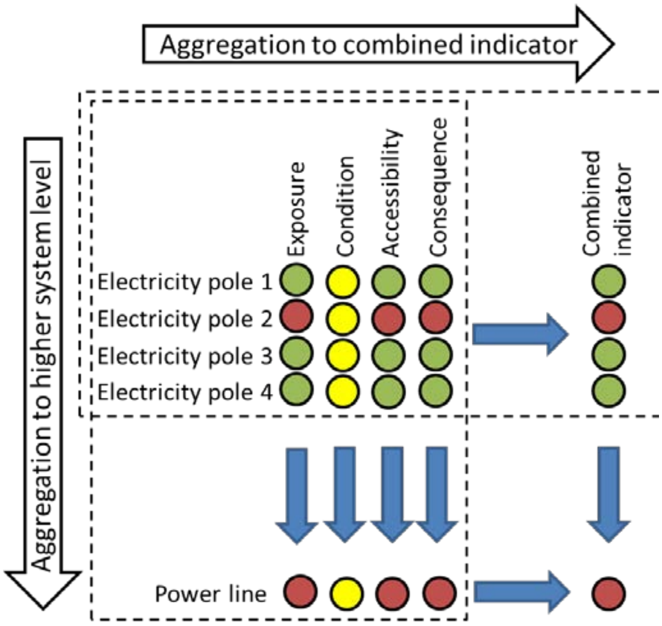


Figure 5-2 Approaches for indicator aggregation.

In the case studies, the different indicators are aggregated to indicators for the whole power line and not only per electricity pole location. The aggregated indicators can be used to give a snapshot of the vulnerability situation of the power line and can also be used to understand which vulnerability dimension is most critical. In addition, the four indicators are aggregated to provide a combined indicator for vulnerability. This indicator can identify for especially critical locations in the power line from a vulnerability perspective. Both aggregated indicators can again be aggregated to describe the vulnerability of the power line with only one overall indicator.

There are two main challenges when aggregating indicators. The first is the scale and unit chosen to measure the indicators and the second is to decide on an aggregation rule securing that no crucial information is lost through the aggregation process. The scale used for the indicators is important if several different indicators shall be integrated into one combined indicator. These indicators should have similar scales or scales that can be transformed into a similar scale. However, for the aggregation to a higher system level the scale is not of such importance since no indicators are combined together.

Different aggregation rules can be applied. A typical aggregation method would be to aggregate for example the single condition indicator values from the electricity pole locations to one indicator for the power line by using the average value. However, the average would hide locations that are especially vulnerable in the power line and this information would not be available at a higher aggregated level. Therefore, a weighted average can be the solution. The weight of the indicator values would be determined by their assigned indicator value when using such a method. That means the worst technical condition values would get a higher weight than values representing perfect condition. Another method could be to aggregate only indicator values that apply to a defined filter. For example, the average of indicator values of the ten worst technical conditions. An extreme case of this method would be to take only the worst value. The same aggregation methods can be applied when aggregating different indicators to a combined indicator. Then again the question is if one indicator should get a higher weight or what kind of information one still wants to have represented in the combined indicator. However, when combining different indicators together, it is also important to decide what weight the indicators should have independent from the indicator value.

In the case studies, it is chosen to use weighted average as aggregation rule for both aggregating from pole location to the power line and for combining all four indicators into one combined indicator. The weighting gives a larger weight to low values and therefore it is possible to sustain the information of critical indicator values also on the aggregated level. Otherwise, such critical values could disappear in the large number of poles that have good indicator values. In addition, it is decided that the four different indicators should have the same weight when they are combined, since there is no indication that one of the factors represented by the indicators contributes more to the vulnerability than the other factors. The following formulas summarize the calculations used.

$$V_{Agg,I} = \frac{\sum_{e=1}^{n} V_{I,e} \times W\left(V_{I,e}\right)}{n}$$

$$V_{Comb,e} = \frac{\sum_{I=1}^{4} W_I \times V_{I,e} \times W(V_{I,e})}{4}$$

$$V_{Agg,Comb} = \frac{\sum_{e=1}^{n} V_{Comb,e} \times W\left(V_{Comb,e}\right)}{n} = \frac{\sum_{I=1}^{4} W_I \times V_{Agg,I} \times W(V_{Agg,I})}{4}$$

$$W_1 = W_2 = W_3 = W_4$$

I – Indicator (Exposure, condition, accessibility, consequence), 1...4
E – Electricity pole locations, 1...n
$V_{Agg,I}$ – Value of the aggregated indicator I at power line level
$V_{Comb,e}$ – Value of the combined indicator at location e
$V_{I,e}$ – Indicator value of indicator I at location e
W(V) – Weight dependent on the indicator value V based on the rule presented in Table 5-2
W_I – Weight of the indicator I when combining different indicators

The final indicators are presented in different colour codes to ease the recognition of vulnerable points in the power line and lead the focus straight to the worst indicator values. The colour coding is based on the traffic light colours and red symbolizes an indicator with low values, meaning for example bad technical condition, while green symbolizes a perfect condition. The weights and the colour classes that were chosen for the different indicator values are summarised in Table 5-2.

Table 5-2 Weights for the aggregation method with weighted average and colour coding.

Indicator value	Weight for aggregation	Colour coding
0 - 24	5	red
25 - 49	4	yellow
50 - 74	3	yellow
75 - 99	2	green
100	1	green

5.5 Indicator results

Based on the presented approach, indicators are calculated for four power lines. For each grid operator, a critical power line in the distribution and in the regional network is chosen. The following tables illustrate the results at single pole level for the four indicators and the combined indicator that combines these indicators into one value.

Table 5-3 Pole locations with the lowest combined indicator values in distribution power line of operator A.

Pole ID	Exposure	Condition	Accessibility	Consequence	Combined
xx	40	0	40	20	23
xx	50	0	40	20	24
xx	50	0	40	20	24
xx	50	50	20	20	31
xx	50	50	20	20	31
xx	50	100	20	20	32
xx	50	100	20	20	32
xx	50	100	20	20	32
xx	50	100	20	20	32
xx	50	100	20	20	32

Table 5-4 Pole locations with the lowest combined indicator values in regional power line of operator A.

Pole ID	Exposure	Condition	Accessibility	Consequence	Combined
xx	50	0	80	10	24
xx	50	0	80	10	24
xx	50	0	80	10	24
xx	50	25	80	10	33
xx	50	25	80	10	33
xx	50	25	80	10	33
xx	50	25	80	10	33
xx	50	50	50	10	36
xx	50	50	50	10	36
xx	50	50	50	10	36

Table 5-5 Pole locations with the lowest combined indicator values in distribution power line of operator B.

Pole ID	Exposure	Condition	Accessibility	Consequence	Combined
xx	100	0	40	10	21
xx	100	0	40	10	21
xx	100	0	40	10	21
xx	100	0	40	10	21
xx	100	0	40	10	21
xx	100	0	40	10	21
xx	100	0	40	10	21
xx	100	0	40	10	21
xx	100	0	40	10	21
xx	100	0	40	10	21

Table 5-6 Pole locations with the lowest combined indicator values in regional power line of operator B.

Pole ID	Exposure	Condition	Accessibility	Consequence	Combined
xx	80	0	40	10	23
xx	80	0	40	10	23
xx	80	100	20	10	32
xx	80	100	20	10	32
xx	80	50	40	10	37
xx	80	50	40	10	37
xx	80	50	40	10	37
xx	100	100	40	10	37
xx	80	100	40	10	39
xx	80	100	40	10	39

All indicators are first calculated at electricity pole level and then aggregated to power line level with the aforementioned aggregation rule. The aggregation of the indicators helps to see why a power line is vulnerable. For example, the power line in the distribution grid of operator B is not exposed to weather related threats, but is not in perfect condition and accessibility can be a challenge. The potential consequences are regarded as critical. Such an overview helps to understand where possible activities could help to reduce the vulnerability of the power line.

Table 5-7 Aggregated indicators for the four case studies.

	Exposure	Condition	Accessibility	Consequence	Combined
Distribution power line A	49	92	51	17	41
Regional power line A	50	60	73	10	39
Distribution power line B	100	44	40	10	34
Regional power line B	84	75	65	10	43

5.6 Indicator quality

The quality of the developed indicators is discussed in relation to the five categories relevance, availability, reliability, completeness and ownership as presented in section 3.6.

Relevance (meaning)
The indicators are relevant for the purpose of understanding the vulnerability of a power line with a special focus on the technical condition and climatic threats that can influence the technical condition. It is tried to construct all indicators as simple as possible by using a straight forward scale from 0 to 100 where 100 represents the goal for a positive development of vulnerability (means a reduction of vulnerability). The indicators are suitable to highlight which vulnerability influencing factors need most attention since they have critical values for a particular power line.

Availability
It has been possible to quantify the different indicators based on different data sources and available information. However, data is not available for all indicators and therefore several indicators have to be based on expert assessments. The data that are used for the condition indicator could have better quality. Moreover, the time of the inspections when the data was collected is often not recorded. In addition, the history of the data is lacking, thus, it is only possible to give a snapshot of the technical condition.

Reliability
The reliability of the data and information used for assigning values to the indicators is regarded as high. The collection of the data for the condition indicator is carried out by inspections where detailed check lists are followed. Thus, this data can be regarded objective. However, the assumptions used to apply the data and information are more questionable. The application of the data collected by inspections for the condition indicator is not straight forward and several simplifications need to be done. For example, the severity of the deviations reported from the inspections does not necessarily correspond to a higher severity in terms of vulnerability. The qualitative information given by maps and experts is also translated to numerical values. This process is still quite arbitrary and needs more thorough analysis.

Completeness
The final set of indicators is complete in the sense that all dimensions of vulnerability are covered and indicators are developed with a focus on the technical condition of the power lines and the threats that

influence the technical condition. However, more indicators are needed to give a complete picture of, for example, the coping capacity and the criticality of the consequences.

Ownership
It cannot be stated that the indicators are trusted and accepted by the grid operators as this has not been a main goal of the indicator development. The case studies are used to illustrate the indicator development process and to gain experience by constructing indicators based on real data.

5.7 Methods for designing leading indicators

One of the main challenges regarding vulnerability indicators is the development of quantitative leading indicators. Two different approaches are identified for developing leading indicators:

- detailed modelling
- external drivers

A leading indicator based on detailed modelling approach uses models that estimate a future value for a given indicator based on changes in underlying factors for that indicator. Examples of underlying factors may be failure history, technical condition and age distribution at the component level. In many cases, these underlying factors are also based on specific models to predict how they will develop in the future. The challenge with this approach is on the one hand, to determine the dependencies of the indicator on the different underlying factors in such a way that these dependencies can be modelled, and on the other hand, that the future development of all underlying factors has to be modelled in addition. Figure 5-3 illustrates the approach for establishing an indicator for the condition of a power line.

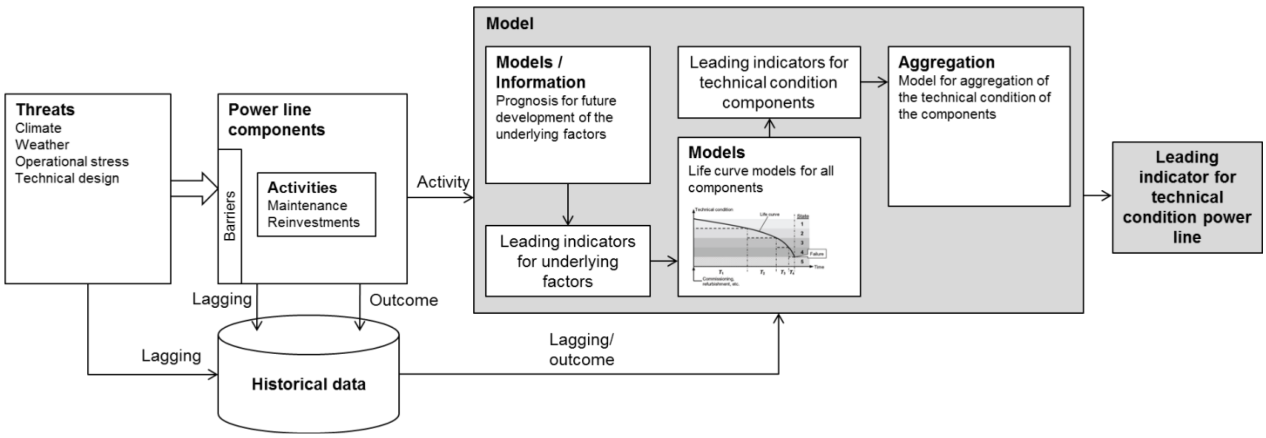


Figure 5-3 Example of leading indicator for the condition of a power line based on detailed modelling of life curves.

In this example, the underlying factors are the climate and the weather of which the components of the power line are exposed to. In addition, the operational stress and the technical design criteria of the components have an influence on the technical condition. The maintenance and reinvestment activities are another underlying factor. The status of these factors can be monitored by lagging, activity and outcome indicators. This information is used into a model to calculate a leading indicator for the technical condition of the power line. The final leading indicator is constructed in several steps. First of all, different models and information should be applied to transform the lagging indicators of the underlying indicators to a future development of these factors. Based on the leading indicators and life curve models for all the components of the power line that are based on the underlying indicators, leading indicators for technical condition of the components can be constructed. Finally, the component indicators must be aggregated to a leading indicator for the power line.

In an approach based on external drivers, the changes in vulnerability are not modelled in detail. This approach focuses on drivers that affect the vulnerability. Such an approach will give prognoses for external drivers and the projections may be based on climate models, general projection models or expert assessments. Underlying factors for the detailed modelling approach and external drivers will often be equal. In the example of the technical condition of the power line, several underlying factors can be understood as external drivers, as for example the climate and weather the power line is exposed to. As in the detailed modelling approach, leading indicators of these external drivers must be calculated. The projected drivers should further be combined into one leading indicator that presents an expected development of the technical condition of the power line, see Figure 5-4.

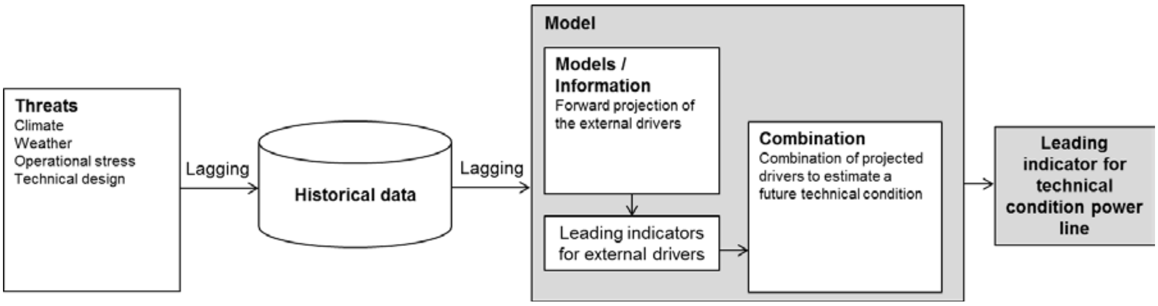


Figure 5-4 Example of leading indicator for condition of a power line based on external drivers.

A major difference between the two approaches is the required amount of data and knowledge about factors that influence vulnerability. The detailed modelling approach requires a large amount of data and models. Examples are lifetime curves and the current condition state for all relevant components for calculating an indicator for technical condition. In addition, a profound knowledge of the relationship between the underlying factors and different failure mechanism is needed to model lifetime curves. On the other hand, leading indicators based on the external drivers approach need only data about external drivers that can be easily available as well as the future projection of these drivers. Information about the influence on vulnerability from these factors is needed, however, only at a general level since no detailed modelling is required.

A general conclusion regarding the approach for leading indicators is that the detailed modelling approach based on for example life curves for all components is not feasible due to the amount of models and data needed. It is more realistic to apply the approach based on external drivers. The different drivers can be projected based on different methods. Figure 5-5 shows a simple example of linear projection of data for the number of lightning strikes in a specific area. However, the relation between the external driver and the vulnerability of the power line still has to be specified and is the missing link to relate the external drivers to for example the technical condition.

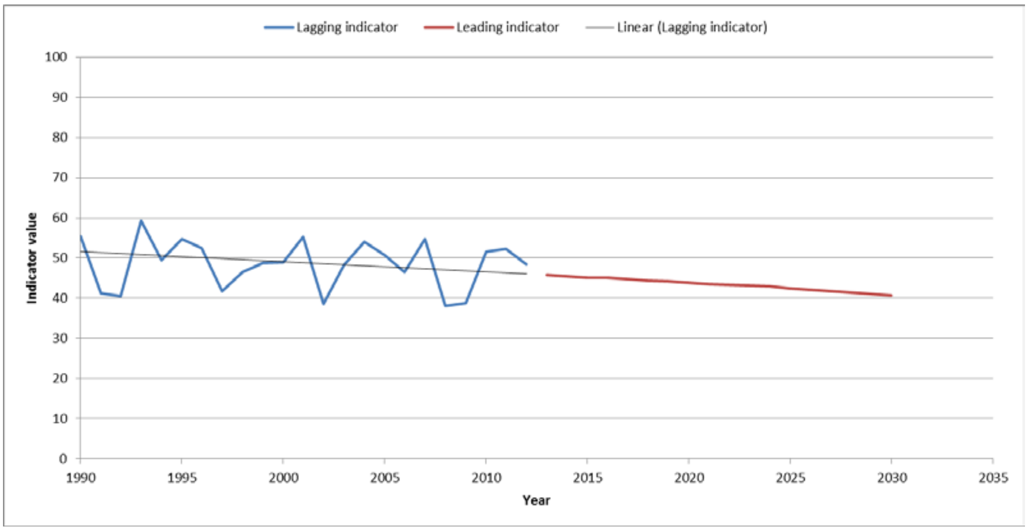


Figure 5-5 Example of linear projection of a lagging indicator.

6 Discussion

One experience from the case studies is that the needed data often is unavailable in the required quality to assign values to the indicators at electricity pole level. The applied data is collected by inspections that identify needed maintenance actions at the electricity poles. The transformation of this data to information that describes the technical condition of an electricity pole which is relevant for vulnerability is not straight forward. In the presented approach, a simple rule reducing the condition for each reported deviation from a start value of 100 has been used. This could lead to instances where the condition is negative. Therefore, it is discussable how close this approach is to reality and other methods or values for calculating a condition index should be tested.

Besides the technical condition indicator, most of the indicator values are assigned based on subjective assessment. A data based approach for quantification of the indicators would be preferable to allow for a fast update of the indicators when new data is available and to use the method more quickly for several power lines. In addition, the specification of weights for aggregation has quite an influence on the final results. The weights used for aggregation in the case studies have been chosen arbitrarily and should be subject to a more thorough analysis. Ideally, weights should be chosen in a way that the aggregated indicators receive values as expected from an expert user. This means that if an expert would characterize an aspect as highly vulnerable, the aggregated indicator values should reflect this. The visualisation with colour codes is an easy method to present the indicators in a user friendly way and it helps to identify critical indicator values right away.

Leading indicators have not been part of the case studies due to the lack of models that could be used to estimate them. The remaining challenge is therefore, to construct such indicators which can be used as an estimate for future vulnerability. However, two different approaches are described at the theoretical level and it seems as the approach based on external drivers is most promising since it only requires a limited amount of data and models for constructing a leading indicator. The main challenge of this approach is to specify the influence of the external drivers on the vulnerability and to determine how the external drivers should be combined into one indicator.

7 Conclusions and further work

This report describes a framework and process for developing vulnerability indicators for electric power grids. It shows in addition how the development process can be applied and some example indicators and theoretical approaches for developing leading indicators are presented. Based on the experiences from the case studies and the theoretical framework the following conclusions can be drawn:

- It is possible to measure vulnerability with indicators.
- Vulnerability of power grids is a highly complex and multi-dimensional topic. To describe the complete vulnerability picture it is necessary to develop and combine a set of indicators that reflect the most relevant vulnerability aspects.
- This project provides examples of indictors that were tested on data provided by two grid operators; however a consistent and complete set of indicators that can be applied to all grid operators is still missing. More research efforts are needed for further development of a set of indicators that represent the whole vulnerability picture of the electric power grid.
- Aggregation and weighting of indicators should be subject to a more thorough analysis.
- Approaches for developing leading indicators are available. However, the development of such indicators is still a main challenge requiring knowledge of the relationship between the external drivers and vulnerability and models for projections.

Further work should be devoted to the development of a consistent set of indicators that covers the complete vulnerability picture for a given part of the electric power grid. The selection of the indicators should be performed in close cooperation with interested parties as grid operators and authorities. In addition, the value assessment for these indicators should mainly be based on available data sets. Therefore, it should be identified what information must be collected. If information is missing, it has to be decided if the higher quality of the vulnerability indicators justifies the costs to obtain the data. A complete case study with the application of these indicators is a prerequisite to highlight the benefits of vulnerability indicators. In addition, leading indicators should be developed with the approach based on external drivers.

8 References

1. Hofmann, M., Gjerde, O. and Kjølle, G., *Vulnerability in electric power grids: State of the art and framework for vulnerability indicators*, *Technical report TR A7120*. 2011, SINTEF Energi: Trondheim.
2. Kjølle, G., et al., *Vulnerability of electric power networks*, in *NORDAC 2006*. 2006, Stockhom.
3. Hofmann, M., Kjølle, G. and Gjerde, O., *Development of Indicators to Monitor Vulnerabilities in Power Systems*, in *PSAM11 & ESREL 2012*. 2012, Helsinki.
4. Thywissen, K., *Core terminology of disaster reduction - A comparative glossary. In: Measuring vulnerability to natural hazards*. 2/2006.
5. EU Commision, *On a European programme for critical infrastructure protection. Green Paper*. 2005, Brussel.
6. OECD, *Guidance on safety performance indicators*, in *OECD Environment, Health and Safety Publications. Series on Chemical Accidents*. 2003, Paris.
7. Lenz, S., *Vulnerabilität kritischer Infrastrukturen. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)*. 2009, Bonn.
8. International Risk Governance Council (IRGC), *White paper on managing and reducing social vulnerabilities from coupled critical infrastructures*, IRGC, Editor. 2006.
9. Kjølle, G., Utne, I.B. and Gjerde, O., *Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies.* Reliability Engineering & System Safety, 2012. 105: p. 80-89.
10. Kjølle, G., *Sårbarhetsindikatorer (og indikatorer for forsyningssikkerhet)*, *Project memo AN 08.12.50*. 2009, SINTEF Energi: Trondheim.
11. Doorman, G., et al., *Vulnerability of the Nordic power system*, *Technical report TR A5962*. 2004, SINTEF Energi: Trondheim.
12. Kjølle, G. and Kyte, R.H., *Dealing with major storms in asset management*, in *NORDAC 2012*. 2012, Helsinki.
13. Kjølle, G. and Kyte, R.H., *Major storms – main causes, consequences and crisis management*, in *CIRED*, CIRED, Editor. 2012, Stockholm.
14. Kjølle, G., Gjerde, O. and Hofmann, M., *Monitoring Vulnerability in Power Systems. Extraordinary Events, Analysis Framework and Development of Indicators*, in *PMAPS*. 2012, Istanbul.
15. Johansson, E., et al. *Extraordinary events - understanding sequence, causes and remedies*, in *ESREL 2010*, Rhodes.
16. Kjølle, G., Gjerde, O., and Nybø, A., *A framework for handling high impact low probability (HILP) events*, in *CIRED Workshop*. 2010.
17. Kjølle, G.H., Gjerde, O. and Hofmann, M., *Vulnerability and security in a changing power system*, *Technical report TR A7278*. 2013, SINTEF Energi: Trondheim.
18. OED, *Utvikling i risikonivå – norsk sokkel. Pilotprosjektrapport 2000 Sammendrag*, Oljedirektoratet, Editor. 2001, Oslo.
19. Vinnem, J.E., *Risk indicators for major hazards on offshore installations.* Safety Science, 2010. Science 48 (6): p. 770–787.
20. Reiman, T. and Pietikäinen, *Indicators of safety culture – selection and utilization of leading safety performance indicators*. 2010, VTT, Technical Research Centre of Finland.

21. Hopkins, A., *Thinking about process safety indicators.* Safety Science, 2009. 47(4): p. 460-465.

22. Statens Energimyndighet, *Guide till indikatordjungelen: Indikatorer inom energiområdet*, in *ER 1:2002*. 2002: Eskilstuna

23. Sand, K., *Risk indicators for distribution systems asset management*, *Teknisk rapport TR A6787*, 2009, SINTEF Energi: Trondheim.

SINTEF

Technology for a better society

www.sintef.no