INDICATORS TO MONITOR AND MANAGE ELECTRICITY DISTRIBUTION SYSTEM VULNERABILITY

Oddbjørn GJERDE
SINTEF Energy Research – Norway
Oddbjorn.Gjerde@sintef.no

Gerd H. KJØLLE
SINTEF Energy Research – Norway
Gerd.Kjolle@sintef.no

Johan G. HERNES
NTE Nett – Norway
Johan.Hernes@nte.no

Birger HESTNES
Directorate for Civil Protection and Emergency Planning – Norway
Birger.Hestnes@nek.no

Jan A. FOOSNÆS
NTE Nett - Norway
Jan.Foosnaes@nte.no

ABSTRACT

This paper describes how indicators to monitor and manage distribution system vulnerability can be identified and established. The process is based on the bow-tie framework for vulnerability analysis, structuring threats, unwanted events, consequences and barriers. Relevant vulnerability indicators are those able to provide adequate information about vulnerability prior to events and the development of vulnerability. Indicators like technical condition of components and system should be combined with weather forecast and other indicators measuring e.g. emergency preparedness, to create an overall picture of the vulnerability towards a certain threat or hazard.

INTRODUCTION

Controlling vulnerabilities related to ageing assets, increasing climatic stress and increased utilization of components etc. is an essential part of distribution system asset management. Previous studies have revealed that there is a need for new knowledge for monitoring and managing vulnerability in the electricity system, e.g. [1, 6]. The best available database for documenting the development of the reliability of supply is the failure and interruption statistics. However, these data only contain information about current components and those that have failed. Presently there are few, if any, indicators and data on an aggregate level to monitor and describe the vulnerabilities in quantitative terms, and to identify e.g. underlying mechanisms impacting the technical condition of the network.

An ongoing research project seeks to reduce this gap by developing methods and indicators to identify vulnerabilities related to wide-area interruptions with severe impact on society. The work is performed in collaboration with Norwegian network companies, the transmission system operator, the energy regulator and electrical safety authority.

Analysis and identification of barriers to prevent or limit the consequences of extraordinary events (low probability, high impact events), provides useful information for the identification of needs for indicators to monitor vulnerability, including indicators providing information about the presence of threats or hazards, potential consequences, and the existence and adequacy of barriers.

This paper describes how needs for indicators to monitor and manage distribution system vulnerability can be identified and indicators established, and how different indicators can be combined to describe a system's vulnerability towards certain threats or hazards. A case study from a small Norwegian island is presented, giving examples of barriers and indicators for a selected type of unwanted event.

ANALYSIS FRAMEWORK AND NEED FOR INDICATORS

The framework is based on the bow tie-model for vulnerability[1] analysis, describing the relations between main causes and consequences of an unwanted event [5]. An example is given in Figure 1 below. The main unwanted events to be considered here are power system failures and the consequences in terms of wide-area interruptions or blackouts. This is shown in the figure below together with major categories of threats.

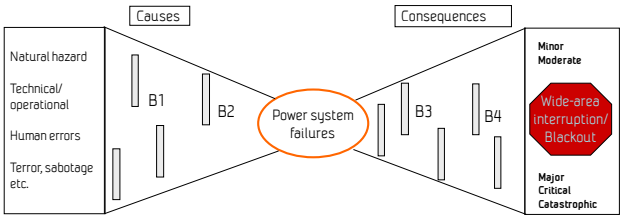

Figure 1 Threats, unwanted event, consequences and barriers [5]

The threats include natural hazard (e.g. a major storm), technical/operational causes (e.g. ageing of overhead lines), human errors (e.g. digging) and antagonistic causes such as

[1] The vulnerability is an expression of the system's lack of ability or reduced ability to withstand an unwanted situation, limit the consequences, and to recover and stabilize after the occurrence of the situation [1].

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

As indicated in the figure, a number of barriers (B1 – B4) exist to avoid threats to develop into unwanted events and to prevent or reduce the consequences. With reference to Figure 1 the barriers can be grouped in four types according to their function as illustrated by examples [5]:

- Prevent component failure (B1)
  - Vegetation management
- Prevent power system failure (B2)
  - Testing of protection settings
- Facilitate restoration (B3)
  - Standardisation of spare parts
- Reduce end-users consequences (B4)
  - Reserve supply units.

A system is vulnerable towards a threat when [7]:

- There is a potential for severe consequences, and
- There are an insufficient number of barriers or the existing barriers have weaknesses, i.e. they may fail to function as intended.

Thus, in order to describe vulnerability, there is a need for indicators providing information about the presence and development of threats, potential consequences, and the existence and adequacy as well as development of barriers.

VULNERABILITY INDICATORS

In the process of establishing good indicators, core questions to be addressed in general include:

- What is the purpose of the indicator?
  - To be used at company, regional or national / international level?
  - For strategic, planning or operation purposes?
- Which types of threats and vulnerabilities to measure?
- What kind of data and models are required?

In addition, indicators must meet certain criteria, e.g. (adapted from [2]):

- Linked to given target(s)
- Reflecting important aspects and development of the vulnerability
- Clearly defined and easy-to-understand
- Possible to measure, e.g. based on official statistics
- Traceability regarding sources of information and how the indicator is constructed.

Different types of indicators

A wide range of different types of indicators are found in the literature. An appropriate categorisation of indicators is as follows [3]:

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

These categories are partly overlapping. The various types of indicators give different and complementary information and it will be necessary to combine indicators for different purposes.

Outcome versus activity based indicators

According to [4] outcome and activity based indicators can be described as follows:

- *Activity indicators* are designed to help identify whether actions believed to lower risks are taken. *Outcome indicators* are designed to help measure whether such actions are, in fact, helping to meet certain targets.
- *Outcome indicators* tell you whether or not you have achieved a desired result, while *activity indicators* tell you why the result was achieved or why it was not.

The distinction between activity and outcome indicators may be particularly useful if one is interested in "measuring" the effect of dedicated activities. This is illustrated in Table 1 which shows examples of indicators related to activities. Note that the activity indicators are easy to observe and relate to goals / activities, while the outcome indicators will be observed over a longer period of time and will usually be a result of many different activities, as well as stochastic factors such as weather.

Table 1 Examples of Activity and outcome indicators

Activity	Activity indicator	Outcome indicator
Vegetation management	Areas/ km with veg. management per year. Costs.	Number of failures per year related to vegetation.
Testing and verification of protection settings	Number/ share of units tested per year. Costs.	Number of failures related to protection failures per year.
Standardisation of spare parts	Number of different spare parts in stock	Average restoration time
Reserve supply units	Number/ capacity of reserve supply units and prepared points of connection.	Average interruption duration. Energy not supplied per year

Leading versus lagging indicators

In general leading indicators are providing information about development of vulnerability, while lagging indicators are providing information about performance in the past. Leading indicators are closely related to activity indicators and lagging indicators are closely related to outcome indicators.

Considered on a time scale, lead indicators will typically precede lag indicators. Regarding power system vulnerability a leading indicator will need to be based on technical condition of the components and system, while fault statistics is a typical example of a lagging indicator. Using the Steigen-blackout in 2007 [5] as an example, the number of faults and energy not supplied (ENS) are shown in Figure 3. It is obvious that studying only fault statistics before 2007 could not have revealed what was about to

happen this year – there is no indication at all in these data. On the other hand, e.g. condition information for the power lines could in this case have been useful for providing a leading indicator.

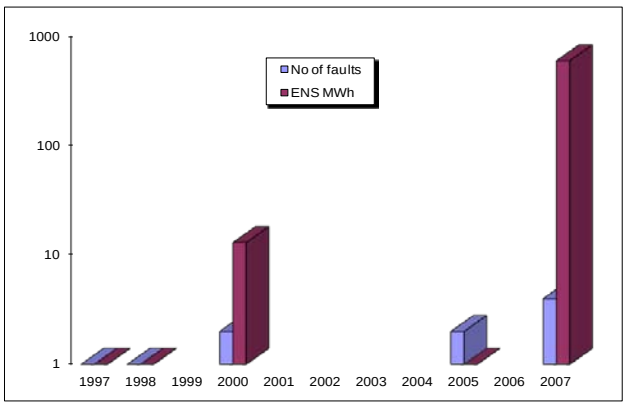

Figure 3 Fault statistics for 66 kV overhead lines

Distribution system vulnerability indicators

To be able to monitor and manage electricity distribution system vulnerability, ex-ante information about threat exposure, possible events and potential consequences is crucial. Based on studies of literature, analyses of historical events and case studies [5] it has been possible to identify needs for vulnerability indicators. Such indicators should say something about the presence and magnitude of threats and consequences and the development of these, as well as the presence, adequacy and development of barriers.

The following list gives examples of barriers important to provide information about in terms of various indicators:

- Dimensioning criteria, components
- Quality of construction work
- Presence of components with inadequate design
- Vegetation management adequacy
- Degree and quality of condition monitoring
- Condition-based indicators for selected components
- Emergency preparedness, including personnel and material availability for restoration
- Availability of communication system in emergency situations
- Quality of risk and vulnerability analyses, plans, procedures, clarification of responsibilities.

Such information must be combined with knowledge about threats, consequences and criticality of components, systems and functions. Weather indicators are particularly important in the context of vulnerability since increasing climatic stress increases the threat, at the same time as system restoration may become more difficult.

It is a challenge to establish good leading indicators, i.e. indicators which say something about vulnerability prior to events, and the development of vulnerability. Sources of information include technical data and information about components condition and experiences from emergency training (preparedness) etc. Analysis of past events and historic data can give valuable insight. Needs for vulnerability indicators are illustrated by a case study in next section.

CASE STUDY

This case study focuses on identification of vulnerability indicators for the power distribution system supplying a small island in Norway. The island is single sided fed from a 66/22 kV transformer at the mainland, via a 22 kV overhead line and sub-sea cable.

The distribution system operator has carried out a risk and vulnerability analysis. Based on criticality the following unwanted events are identified, as these will all lead to blackout of the entire island:

1. Outage of regional network or 66/22 kV transformer station
2. Failure of 22 kV overhead line
3. Failure of sub-sea cable.

The unwanted event number three, “failure of sub-sea cable”, is selected for identification of barriers and need for vulnerability indicators. Figure 4 shows the corresponding bow-tie model with threats, causes, barriers and consequences.

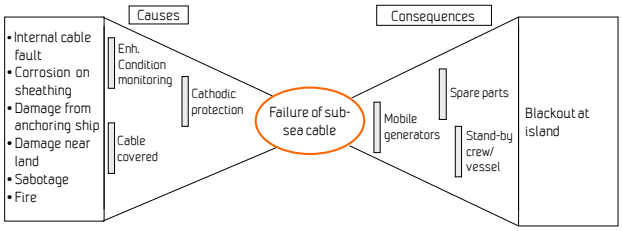

Figure 4: Bow-tie for failure of sub-sea cable.

The causes may be divided into major groups as shown in Figure 1 ”natural hazard”, ”technical/ operational”, ”human errors” and ”terror/ sabotage”. Figure 4 shows the relevant subgroups of causes for failure of sub-sea cable.

The risk and vulnerability analysis identified the following implemented barriers against threats:

- The cable is buried where coming on-shore at both ends
- Enhanced condition monitoring is implemented
- Cathode protection is installed to avoid corrosion.

The following implemented barriers against consequences are identified:

- Mobile generators for up to 100% of the load are available within specified time frames
- A selection of spare parts for repairing sub-sea cables

are on stock
- Repair personnel are available within specified time.

For the unwanted event "failure of sub-sea cable" the identified barriers belong to three different groups in this case:

1. Condition of sub sea cable
2. Preparedness
3. Weather – influences restoration of supply.

As described in the vulnerability analysis framework the need for indicators are strongly linked to barriers. Table 2 shows different possible vulnerability indicators for the power supply to the island, related to failure of the sub-sea cable. In the table a scale for measuring the indicator is suggested, as well as the category it belongs to.

Table 2 Vulnerability indicators – failure of sub-sea cable

Indicator	Scale	Type
Weather forecast		Leading
Overall technical condition of cable	Condition class	Leading
Visual impression, damages and coverage near shore		Leading
Fault history for current cable	Faults/year	Lagging Outcome
Quality of supply at island	Number of interr./ ENS/ restoration time	Lagging/ outcome
Capacity of available mobile generators	% of load	Leading Activity
Spare parts in stock		Leading Activity
Qualified work force available for repair (incl ship transport)		Leading Activity
Risk and vulnerability analyses carried out	Yes/no	Leading Activity

Leading indicators as listed in the table above are related to technical condition of the sub-sea cable, meaning that information about the condition will be important to establish a leading indicator to monitor vulnerability. Weather forecast is clearly important in this case, and may also be regarded as a leading indicator although the "lead" in terms of time ahead may vary. The table also shows that the different types of indicators partly overlap, e.g. the fault history for the cable gives the outcome regarding faults per year in the past which can be regarded as lagging information.

It is believed that combining various activity and outcome indicators, as well as leading and lagging indicators, a picture of vulnerability of the power supply to the island can be established.

When in addition risk and vulnerability analyses are carried out, this establishes a good basis for emergency preparedness including need for information flow and coordination, as well as establishing and modifying other barriers both at cause and consequence sides.

CONCLUSIONS AND FURTHER WORK

This paper has shown how needs for indicators to monitor and manage distribution system vulnerability can be identified and indicators established based on the bow-tie framework for vulnerability analysis. The framework structures threats, unwanted events, consequences and barriers.

The need for vulnerability indicators are closely related to information about threats, consequences and the existence and adequacy of barriers. Relevant vulnerability indicators say something about vulnerability prior to events, and the development of vulnerability (leading indicators). Through a case study it is shown how different vulnerability indicators can be found for an unwanted event (failure of a sub-sea cable).

Indicators like technical condition of components and system should be combined with weather forecast and other indicators like emergency preparedness to create an overall picture of the vulnerability towards a certain threat or hazard.

Further work will emphasise establishment of various types of vulnerability indicators and specify content, e.g. scales for measurement and data needed. It is also necessary to elaborate further how to combine the indicators of various types into an overall picture of vulnerability development, how to compare the vulnerability for different systems and rank it, and how to compare and rank the effect of different vulnerability reducing measures.

REFERENCES

[1] G. Doorman et. al., 2004, *Vulnerability of the Nordic power system*, SINTEF Energy Research, Trondheim

[2] Statens Energimyndighet, 2007, *Indikatorer för försörjningstrygghet*, ER 2007:04, Eskilstuna (in Swedish)

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

[4] OECD, 2003, *Guidance on safety performance indicators*, OECD Environment, Health and Safety Publications, Series on Chemical Accidents, Paris

[5] G. Kjølle, O. Gjerde, A. Nybø, 2010, "A framework for handling high impact low probability (HILP) events", *CIRED workshop*, Lyon

[6] G. Kjølle, K. Ryen, B. Hestnes, H. O. Ween, 2006, "Vulnerability of electric power networks", *NORDAC* 2006, Stockholm

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