Critical infrastructures and risk analysis of electricity supply

G. H. Kjølle
SINTEF Energy Research, Norway

I. B. Utne
Norwegian University of Science and Technology, Norway

ABSTRACT: Failures in critical infrastructures can cause major damage to society, and thus there is a need for a common approach to cross-sector risk analyses. This paper presents such an approach, which includes an extended preliminary hazard analysis and detailed risk analysis of electricity supply, carried out in a case study. The risk analysis approach constitutes an important basis for analyzing interdependencies between sectors and assessing overall risks of failures in critical infrastructures. The case study results show that the approach is a promising starting point for risk analysis of electricity supply interruptions and the consequences for dependent infrastructures.

1 INTRODUCTION

The modern society is critically dependent on a secure electricity supply to maintain its functionality. Due to this dependence, the electricity system is defined as one of society's critical infrastructures (EU 2005, NOU 2006). Wide-area interruptions of electricity supply (blackouts) have severe impacts on societal critical functions and need to be addressed from a societal point of view. Beyond the traditional and deterministic N-1 criterion used in electric power systems, there is no agreed-upon framework on how to analyze and predict the security of electricity supply. In risk analyses of electric power systems, a major challenge is to identify possible chains of events that could lead to wide-area interruptions, and to further identify the consequences of these cascading outages. This paper focuses on the effects of blackouts on electricity supply to delivery points, such as other critical infrastructures.

In the last two decades, a simple approach to quantitative risk analysis called ROS (In Norwegian: "Risiko- og sårbarhetsanalyse") (DSB 1994), corresponding to risk and vulnerability analysis, and resembling preliminary hazard analysis (PHA) (Ericson II 2005), has been applied and adapted for different critical infrastructure sectors. This has resulted in various independent risk assessment approaches, and, for instance, insufficient analyses of interdependencies between the different sectors.

There are different kinds of safety and security challenges that critical infrastructures have in common, such as climate changes/natural disasters, ageing (in capital intensive infrastructures like water and electricity supply), restructuring and outsourcing, terrorism, and globalisation. There are also some interdependencies, e.g., between electronic communication and the electric power system (NOU 2006). The challenges need to be dealt with through in-depth sector studies and interdisciplinary studies across sectors, e.g., to develop methodologies for comparisons and exchange of best practices.

In a recent research project, a cross-sector risk analysis approach was developed and tested for this purpose, including the critical infrastructures electricity supply, water supply, transport (road/rail), and information and communication systems (ICT). The main focus was on serious events, emphasizing interdependencies between the sectors. In short, the approach includes an extended PHA and detailed analyses of specific hazardous events in critical infrastructures. A case study of the city of Oslo, Norway, was carried out to test and improve the method, and this paper presents the results from the detailed analysis of a main event occurring in the critical infrastructure electricity supply. The analysis is based on simulations of outages in the electric power system using methods for contingency analysis (power flow) and reliability analysis of power systems.

The first part of the paper describes the cross-sector risk analysis approach, including the extended PHA for critical infrastructures. Next, the detailed risk analysis of electricity supply that was carried out in the case study is presented. The immediate results are number of interruptions of electricity supply, interruption duration, and energy not supplied for each delivery point. Further, consequences for other infrastructures may be pursued.

2 A CROSS-SECTOR APPROACH TO RISK ANALYSIS

A cross-sector approach enables risk analysis of several infrastructures at the same time, which provides useful information for planning emergency preparedness, identification of vulnerabilities, and prioritization of risk reducing measures across sectors. In addition, a common approach (which may as well be used for each sector individually) enables comparison of results for the different critical infrastructures.

The approach presented in this paper consists of four main steps and several tasks, further discussed in subsequent sections:

1 *Planning*
   a) Clarification of objectives and stakeholders
   b) Definition of system boundaries per sector
   c) Establishment of forum for relevant stakeholders
2 *Preliminary Hazard Analysis*
   a) Definition of consequence dimensions
   b) Identification of main events affecting different sectors
   c) Identification of societal critical functions (SCF) relevant for the events
   d) Evaluation of frequency and consequence according to categories, and use of risk matrices
3 *Detailed analyses*
   a) Selection of main events for detailed analyses, based on the results from step 2
   b) Description of accident scenarios and the systems subject to detailed analyses
   c) Performing detailed analyses, e.g., causal analysis, consequence analysis and interdependency analysis
4 *Total assessment of overall risk*
   a) Evaluation of risks across sectors
   b) Planning for implementation of risk reducing measures (and identify needs for further analyses)

2.1 *Step 1 - Planning*

Planning of work ensures that the analysis meets the objectives (Rausand & Utne 2009). Objectives are usually dependent on stakeholders, who should be identified as part of the initial planning process.

Stakeholders may have various motives; for example, municipalities may be preoccupied with getting a total overview of vulnerabilities across infrastructures to plan emergency preparedness, whereas infrastructure owners may be more concerned about analyses of production and availability of services. Users may want to assess their dependencies to critical infrastructures and their need for back-up solutions.

The scope of the analysis is important to determine, for example, if the analysis concerns the infrastructures at an overall system level, or at subsystem or single component level, such as grid transformer stations related to electricity supply. Other important issues are to determine what kind of consequences should be included, for example, service availability, harm to human health, human fatalities, and damages to assets; and to what extent the analysis should include human and organizational contributions, and malicious acts.

To facilitate exchange of knowledge and stakeholder discussions about risk perceptions, a forum for relevant stakeholders should be established. Such a forum must also include system experts.

2.2 *Step 2 – Preliminary hazard analysis (PHA)*

The PHA in the cross-sector approach is rather extensive, compared to a “typical” PHA (Ericson II 2005). It includes identification of hazardous or main events and analysis of risks in a rather coarse way. Extensions are, among other things, linkage between societal critical functions (SCF) and the main events that may occur in the critical infrastructures. The SCFs are used to distinguish between the critical infrastructures and their functions in society. This distinction helps focus on the purpose of the infrastructures and analyze their system constituent parts.

The first task of the PHA is to define the consequence dimensions, based on discussions in the stakeholder forum. Examples of such dimensions and their categories are shown in Table 1, but these have to be adapted to the specific situation at hand.

Table 1. Consequence categories (examples)

Category	Life and Health	Economy
1	Up to 5 injured/ seriously ill	< 1 mill. NOK
2	6-40 injured/ seriously ill	1-10 mill. NOK
3	1-2 fatalities, 40-100 injured/ seriously ill	10-100 mill. NOK
4	3-10 fatalities, 100-500 injured/ seriously ill	100-1000 mill. NOK
5	More than 10 fatalities, more than 500 injured/ seriously ill	>1000 mill. NOK

When the consequence dimensions have been defined, the main events have to be identified and described. The main event description may be supplemented by either a general or a site specific description, included if there is a gross accident potential, if there are communication challenges to the public, and how the main events may impact the SCFs. This means that the SCFs affected by the event should be analyzed in terms of if they “acted” before the main event occurred, i.e., that failure in one SCF leads to the main event, if the SCF was threatened/impacted by the main event, or affected after the event. Examples of SCFs are electricity supply, electronic communication, water and sewage supply, social security services, and emergency- and rescue services. An example showing parts of the hierarchical structure of one SCF is shown in Figure 1.

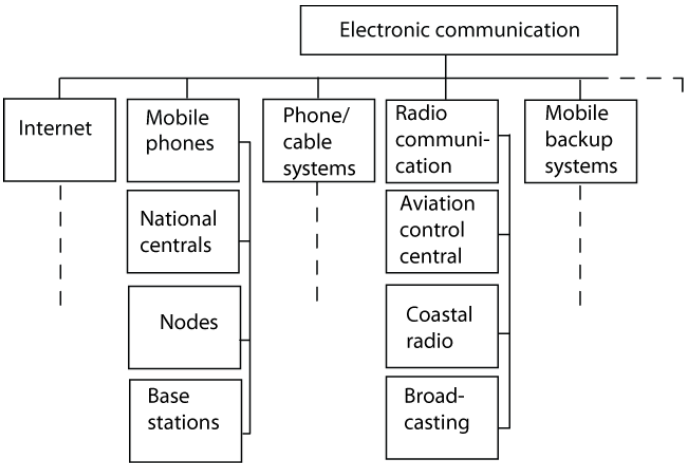

Figure 1. The SCF hierarchy electronic communication, which is related to the critical infrastructure ICT

To assess the risk of the main events, categories for probabilities and consequences are established. In Table 1, categories 1-5 are used for consequences; 1 representing the "best" outcome and 5 the "worst". To calculate the frequencies, a two step procedure is used. Initially, the probability of the occurrence of the main event is assessed. Next, a conditional probability is specified to enable assessment of "worst-case outcomes", i.e., how often or how likely it is that the main event results in a worst case consequence. The conditional probabilities are, for example, related to risk-reducing barriers in the affected infrastructure(s) and external conditions (such as weather conditions). Thus, the probabilities may vary between main events and locations.

Based on the frequency/probability and consequence categories, a risk priority number (RPN) is calculated for the main events, by adding the numbers. A frequency category of 2 and a consequence category of 4, gives RPN= 6.

2.3 *Step 3 – Detailed analyses*

The PHA in step 2 is the first screening process of identifying and analyzing main events affecting critical infrastructures. Some of the main events may have to be analyzed more in detail, due to for example, high risk, serious consequences, strong interdependencies and so on. Before selecting events for further analysis, it is important to clarify the main objectives of the detailed analysis.

A detailed analysis may focus on interdependencies, and possibly include causal analyses (e.g., fault tree analysis (FTA)), and/or consequence analyses (e.g., event tree analysis (ETA) and network flow analysis). The purpose of causal analysis is to identify and assess all possible causes to the main event, whereas the purpose of the consequence analysis is to gain more knowledge about what may happen after the event has occurred and the impact of it.

The first step of the detailed analysis is to transform the selected main events into "accident scenarios". Ericson II (2005) defines an accident scenario as "series of events that ultimately result in an accident. The sequence of events begins with an initiating event and is (usually) followed by one or more pivotal events that lead to the undesired end state". This means that the accident scenario is a detailed description of the main event. Rinaldi et al. (2001) discuss six dimensions of critical infrastructures that may be useful for structuring the accident scenario descriptions.

In a cross-sector risk analyses, couplings or interdependencies between the infrastructures strongly affects the outcome of a main event. In the literature, authors distinguish between different interdependencies. Zimmerman (2001; 2004) uses *spatial* and *functional* interconnectedness and dependency. Spatial interconnectedness describes the proximity between infrastructures as the most important relationship between the systems, e.g., electric power cables and telecommunication cables in the same ditch or culvert. Functional interconnectedness occur when an infrastructure is necessary for operation of another infrastructure; e.g., railway communication system needing electricity in order to function.

In the cross-sector risk analysis approach described in this paper, two categories are applied; (i) location-specific (physical) interdependencies, and (ii) functional interdependencies. The location-specific interdependencies are similar to the spatial interconnectedness of Zimmerman (2001; 2004). Functional interdependencies represent the functions of the systems in the scenario, resembling the functional interconnectedness of Zimmerman (2001). Further description of a cross-sector approach to analyzing risks of interdependencies is found in Utne et al (2009).

2.4 *Step 4 – Risk reducing measures and total risk assessment*

The results of the detailed analysis have to be assessed to determine if the accident scenario(s) may happen in other places, if the accident scenario(s) has higher or lower risks than similar scenarios, and if further analyses are needed. In a cross-sector risk analysis, this means that the results from the detailed analyses have to be integrated into the overall cross-sector analysis, that possible risk-reducing measures should be evaluated, along with those already assessed during the PHA and those directly occurring from the detailed analysis. Assessments of risk reducing measures should include discussions between the stakeholders.

The approach for risk analysis of electricity supply is described in section 3 while sections 4 – 5 describe the cross-sector risk analysis approach carried out in a case study, for a main event occurring in the critical infrastructure electricity supply.

3 RISK ANALYSIS APPROACH FOR ELECTRICITY SUPPLY

3.1 *Power system failures and hazardous events*

The electricity system is an extremely complex and comprehensive infrastructure. Despite of the numerous components of the system and the complexity, the electricity system is very robust and reliable. However, power system failures occur occasionally in the main grid, as well as in the regional and local networks, most often with minor consequences. While the electricity system on the main grid level (and regional) is usually dimensioned and operated according to the N-1 criterion, meaning that the system should withstand loss of a single principal component without causing interruptions of electricity supply[1], local networks are mostly operated as radials and any component outage due to a failure will lead to interruption of electricity supply.

Severe consequences of interruptions, such as loss of supply to a district or part of the city, will most likely be caused by combinations of failure events. In some parts of the system there are location-specific (spatial) dependencies, such as two power lines on the same tower or in the same right-of-way, and cables in the same culvert. There are also functional (inter)dependencies related to the protection and control systems (ICT) etc. In addition, human factors may contribute to cascading events, e.g., inadequate behaviour of operators, and there may be unfortunate circumstances, such as power units being out due to maintenance. Such conditions increase the probability of a system entering an emergency or blackout state.

Hazardous or main events involving coinciding independent or dependent failures happen once in a while and may cause severe impact, but are usually regarded to have low probability.

As far as the electricity system is concerned, probabilistic approaches to reliability evaluation are rather mature, see, e.g., (Billinton et al. 1996; 1999). Generally, these approaches aim to measure the capability of the system to supply the load in the steady state (adequacy) in which the power system may exist considering normal conditions.

There is no established framework on how to analyse and predict the security of electricity supply, meaning the ability of an electricity system to supply final customers with electricity (EU Dir. 2006), and the risk of extraordinary events. A vulnerability analysis of the Nordic power system revealed a lack of knowledge on what is a sufficient or acceptable level of security of electricity supply, and how to analyse extraordinary incidents with low probability and severe impact on society (Doorman et al. 2006).

3.2 *Risk assessment*

For the risk analysis and case study presented in this paper, it was chosen to utilize the well established methodology for reliability analysis of electric power systems, denoted contingency enumeration approach (EPRI 1982). A contingency is an event composed by outages of one or more components due to failures, which may have technical, human or nature related causes. Various contingencies may lead to the main event “loss of electricity supply to a delivery point”. The contingency enumeration approach comprises three main steps:

1 Selection and evaluation of contingencies
2 Consequence analysis of contingencies
3 Reliability assessment and accumulation of reliability indices

In the first step, the objective is to reduce the number of contingencies for detailed analysis. A typical analysis depth is to include all first and second order independent outages, and dependent outages such as common mode, station originated outages or other user-defined outages. In the contingency analysis of the second step, the objective is to identify which delivery points that will experience interruptions (or reduced supply). This consequence analysis is based on simulations of contingencies in the electric power system using physical power flow models. The final step is to perform the reliability analysis and accumulate reliability indices. For this purpose a reliability model is required. The model used here is shown in Figure 2.

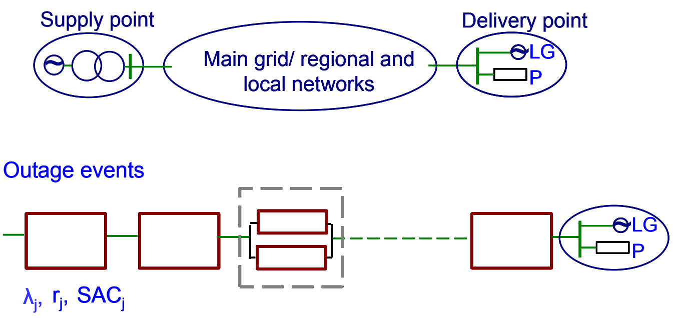
Supply point
Delivery point
Main grid/ regional and local networks
LG
P
Outage events
LG
P
λ_j, r_j, SAC_j

Figure 2 Reliability model for a general delivery point

Where
P = Load in the delivery point (DP)
LG = Local generation at DP
λ_j = Equivalent failure rate
r_j = Equivalent outage time
SAC_j = Available capacity to supply the load after the occurrence of contingency *j*

[1] See for instance the Nordic Grid Code (www.entsoe.eu)

The method combining contingency and reliability analysis is described in (Samdal et al. 2006). The model takes the critical contingencies (outage events) for a delivery point as a starting point. These contingencies are described as a minimal cut-set structure, including those contingencies found to cause problems through the consequence analysis. A cut-set may represent a single component failure or a multiple independent or dependent event as described above. Each cut-set is represented by an equivalent failure rate (λ_j), outage time (r_j) and the available capacity (SAC_j) to supply the load (P) after the occurrence of contingency *j*. An interruption occurs for a delivery point when the total capacity is unable to match the load, i.e., when P > SAC + LG.

The contingency enumeration approach (Samdal et al. 2006) is used for at least one operational state, i.e., a system state valid for one or several months of the year characterised by load and generation composition, including the electrical topological state (breaker positions etc.) and import/export to neighbouring areas.

The contingency and reliability analysis requires various types of data about the power system under study, components, loads and end-users, data from failure statistics, operating procedures, reserve supply possibilities etc.

There is a wide range of reliability indices in use, both delivery point and system oriented indices. The basic delivery point indices are number of interruptions of electricity supply and interruption duration, while the consequences are described in terms of disconnected load and energy not supplied.

Fundamental parts of a risk analysis is to answer questions like 1) What can go wrong, 2) How likely is it to happen, 3) If it happens, what are the consequences? The reliability assessment method presented in this section addresses all these parts for the electricity system. The contingency analysis gives answers to 1) and 3), while the reliability model provides information about the probability or frequency of events 2). Thus, the delivery point indices, such as number of interruptions and energy not supplied can be regarded as risk indices.

4 CASE STUDY

4.1 *Extended preliminary hazard analysis (step 2)*

In the research project it was chosen to perform a case study to facilitate the development of the risk analysis method for critical infrastructures (Utne et al. 2008) and to test this, among other things, in combination with the risk analysis of the electricity supply. The case study was carried out in collaboration with the Emergency Preparedness Group (consisting of critical infrastructure owners) of the city of Oslo and the network company Hafslund Nett. The extended PHA comprised water supply, transportation, electricity supply, and ICT (Utne et al. 2009). The case study focused mainly on serious events involving several infrastructures, and used previous risk analyses of the municipality as a starting point. The analysis covered events of technical character, malicious acts, as well as natural hazards.

A total of 14 unwanted events related to electricity supply were analyzed as a part of the PHA. These events could potentially lead to wide-area interruptions, but none were found to be of high risk related to human life or health, even though they may cause severe economic losses. However, the other infrastructures depend to a large extent on electricity supply and thus it is a challenge to identify consequences for these infrastructures if the electricity supply is interrupted.

Based on the PHA for the mentioned infrastructures, four main events were selected for further detailed analysis. The selection process is described in (Utne et al. 2008). The events or scenarios selected for detailed analysis were:

1 Loss of electricity supply to parts of the city, i.e., to delivery points in the regional network
2 Loss of water supply and consequences for a hospital
3 Fire/explosion at the main aviation fuel storage
4 Joint event in culvert at Oslo central station

This paper focuses on main event 1.

4.2 *Overview of the power system under study*

Figure 3 gives a stylized overview of the electric power system in Oslo. The voltage level of the main grid supplying Oslo is 300 kV, while there are three voltage levels in the regional network in the city; 132 kV, 47 kV and 33 kV. These are mostly underground cable networks but there are also overhead lines. The medium voltage (MV) network mainly consists of 11 kV underground cables.

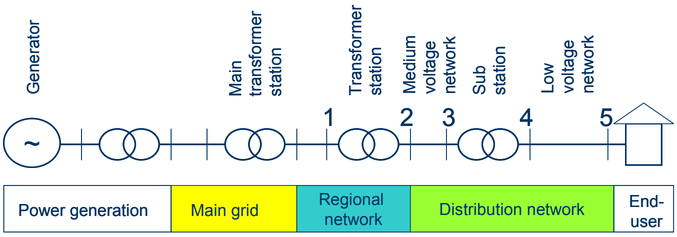

Figure 3 Stylized overview of the power system (value chain) from power generation to demand (source: Hafslund Nett)

According to the network company's interruption statistics for the period 2001 – 2007, the end-users of Hafslund Nett will on average experience an interruption every second year with a duration of 18 minutes due to failures in the regional network. Including failures in the medium voltage (MV) network (level 3 and 4 in Figure 3), the number of interruptions increase to 0,8 per year with an annual duration of 0,7 hours per year. Thus, the regional network contributes to about 50 % of the number of interruptions, while the MV network stands for 60 % of the total interruption duration.

In the same period, there have been three major events in the electricity system in Oslo affecting larger parts of the city. Two of these events (in 2005 and 2007) involved multiple failures and cascading events in the main grid (300 kV), causing loss of one or more main transformer stations and interruption to a major portion of the end-users. Both these events lasted for less than one hour. The third event, at Oslo central station in 2007 (DSB 2008), started as a minor fire in an 11 kV cable caused by digging in the area around the central station. The fire led to evacuation of the station. There were ICT cables in the culvert affected by the fire, and several communication systems were interrupted, including train operation services, internet and phone services. 80000 train passengers and more than 25000 telephone and internet customers were affected. It took 16 hours before the electricity supply was restored and another 4-5 hours before the central station was reopened for the public and the train traffic resumed. This incident involved several interdependencies, described in (Utne et al. 2009).

The statistics and experiences at Hafslund show that major incidents in the past most often have technical or system related causes. The following list shows examples of combinations of events that might result in severe consequences depending on where or when they will occur:

- Breakdown of towers with double lines
- Damage of two or more cables in the same culvert or road bridge
- Fire in various transformers in the same station
- Failure in gas-insulated breaker installations
- Busbar-failure resulting in loss of all lines to and from a transformer station
- Failure in combination with protection system failure, or overlapping maintenance
- Outage of a whole transformer station due to water break-through, construction work a.o.

4.3 *Consequences of hazardous events*

In case of transformer failures (breakdown), it can take months to replace the transformer. The electricity supply will in most situations be restored by reconnection to other parts of the system. There are also possibilities for reserve supply from the underlying MV network. Most of the year there is capacity available to cover the load of the transformer station (at level 2 in Figure 3) even if two failures occur simultaneously.

The contingencies under study in this case are those that have the potential of interrupting the electricity supply to the delivery points in the regional network, i.e. on the secondary side of the transformer station (level 2 in Figure 3). Typical consequences will be:

- Limited outage duration: 0,5 – 1 hour
- Restoration by reserve connections
- A lot of people affected, large economic consequences (e.g. category 3 – 5 in Table 1)

The network company is capable of estimating indices, such as number and duration of interruptions to different delivery points, the amount of interrupted load, energy not supplied (ENS) and the corresponding cost (CENS), as well as area or number of end-users affected. Information about the type of customers is necessary due to the reliability of supply regulation in Norway which adjusts network companies' revenue caps in accordance with the customers' interruption costs CENS (Langset et al. 2001). In this arrangement the individual end-user consequences are represented by average cost rates per customer category (Kjølle et al. 2008). Consequences when loss of electricity supply results in unavailability of dependent infrastructures, public services etc., are however not included in CENS. It is a challenge for network companies to have detailed knowledge about the different end-users behind each delivery point. Interrupted electricity supply to for instance transport, water supply and telecommunication may cause problems for traction power supply, tunnel lighting, pumping systems, marking and control current, base stations for mobile phone systems etc. These consequences need to be investigated separately by the parties being responsible for the operation of the infrastructures.

5 RISK ANALYSIS OF ELECTRICITY SUPPLY – CASE STUDY RESULTS

In this paper, the focus is on the detailed risk analysis considering the loss of electricity supply (blackouts) and the effects on the supply to delivery points, such as other critical infrastructures or to a part of the city, as part of the cross-sector approach. For this purpose the analysis covers the power system from the source (power generation) down to level 2 in Figure 3, i.e., including the main grid, regional network and the transformer stations.

The contingency enumeration approach described in the previous sections was tested for the detailed (quantitative) analysis (step 3 of the cross-sector risk analysis approach) to determine how often a hazardous (main) event will occur (number of interruptions) and the consequences in terms of interruption duration and energy not supplied. It is assumed that this kind of information is useful to operators of dependent infrastructures as a basis for their consequence evaluation and emergency preparedness.

The main event "loss of electricity supply to parts of the city, i.e. to delivery points in the regional network" may be caused by outage of transformer stations and/or power lines in the main grid and regional network in Oslo. The event is critical if it occurs in heavy load situations, usually in cold winter periods. In such situations the reserve capacity is limited. The analysis is made for the heavy load situation only.

Examples of results are given in Tables 2 – 4 for two different transformer stations in the 33 kV network in the inner parts of Oslo city. All failure causes are included.

Table 2. Reliability indices for 33 kV. Single line outages*

Delivery point	No. of interr.	Duration	ENS**
	No/year	Hrs/interr.	MWh/year
Station A	0.12	105	47
Station B	0.07	95	69

* No reconnection possibilities. **ENS = energy not supplied.

Table 3. Reliability indices for 33 kV. Single line and transformer outages and common mode*

Delivery point	No. of interr.	Duration	ENS**
	No/year	Hrs/interr.	MWh/year
Station A	3.0	71	2340
Station B	0.12	371	292

* No reconnection possibilities. **ENS = energy not supplied

Table 4. Reliability indices for 33 kV. Single & double line and single transformer outages. Outage times 1 hour

Delivery point	No. of interr.	Duration	ENS**
	No/year	Hrs/interr.	MWh/year
Station A	0.15	1	0.7
Station B	0.11	1	1.0

**ENS = energy not supplied

As the results are based on the heavy load situation only, the reliability indices are annualized, i.e. the number of interruptions and energy not supplied presented in the Tables 2 – 4, are given in units per year as if the heavy load situation lasts for a whole year. One should keep in mind that the heavy load situation is regarded as worst case, but this situation lasts for only a small portion of the year. This portion could have been used to determine the conditional probability as described in section 2. However, for the emergency preparedness of other critical infrastructures it is important to consider the worst case outcome of interrupted electricity supply.

Table 2 gives results when only single line outages are analyzed, while Table 3 includes both single line and transformer outages, as well as common mode outages. In these two cases presented in Table 2 and 3, reserve connection possibilities are not considered. The common mode failures represent failures in cables in the same culvert or road bridge (spatial dependency). The results show that particularly Station A is affected by such failures giving considerable increase in the frequency of interruptions and energy not supplied. Including independent double line outages, as in Table 4, only gives a small rise in the frequency of interruptions. According to Table 2 and 4, Station A will experience interruption every 6 – 8th year considering single and double independent failures, while it will happen three times a year including also the common mode failures (Table 3). Station A serves some critical societal functions, for instance a hospital. Thus, the consequences of loss of electricity supply and interdependencies to other infrastructures and critical functions should be further investigated.

As mentioned above, reserve connection possibilities are not considered in these two cases presented in Table 2 and 3. This is the main reason for the very large average outage duration for each of the transformer stations. The reliability data are taken from the national statistics, using the expectation (average) values including all failure causes, while there are large dispersions in outage times. To illustrate the effect of reserve possibilities, all outage durations are set to 1 hour in Table 4. This represents the time it will take for the operator to perform reconnections from the control centre. In practice the network company have various possibilities for provisional restoration of supply to the delivery points, depending on local conditions. Different measures take different time. For instance, it may take 4 – 24 hours to connect reserve supply from underlying MV network and up to 4 days to move transformers. It is rather complicated to model and take into consideration all such possibilities and procedures in the reliability assessment. These are topics for further development of the contingency enumeration approach, as specified in (Samdal et al. 2006).

Keeping in mind the assumptions and premises for the analysis described above, the results presented are not realistic for the actual electricity system in Oslo. The results should be regarded as examples of typical results that can be provided from the current reliability and risk assessment methodology. This kind of information may be important when pursuing interdependencies and consequences for other critical infrastructures. It is possible from the contingency enumeration approach also to reveal information about which contingencies are critical for each delivery point and their contribution to the reliability indices.

6 CONCLUSIONS AND FURTHER WORK

This paper presents a cross-sector approach developed in a research project and used to analyze risks of critical infrastructures. To visualize the approach, a case study of Oslo was carried out.

The electricity system in Oslo was used to test and provide information about risk of electricity supply interruption. The risk analysis method can be used to estimate how often electricity supply will be interrupted to specific delivery points and for how long. This is important information for the further identification of consequences in other infrastructures, providing a basis for the emergency preparedness planning. The methodology may also give information about area affected, duration, disconnected load, energy not supplied and corresponding societal costs. In addition the risk analysis revealed both spatial and functional dependencies in the electric power system and dependent failures are found to strongly affect the reliability of supply.

In a cross-sector risk analysis it is important to gather sufficient competence and information. The case study provided valuable opportunities for improved communication between stakeholders and infrastructure owners in the Emergency Preparedness Group of Oslo. The results show that the approach is a promising starting point for risk analysis of wide-area interruptions of electricity supply and the consequences for dependent critical infrastructures. However, further work is needed to identify the consequences of interrupted electricity supply to infrastructures, such as transport, water supply and telecommunication, e.g. problems for traction power supply, tunnel lighting, pumping systems, base stations for mobile phone systems etc.

In detailed risk analysis of electricity systems, a major challenge is to identify chains of events that could lead to wide-area interruptions (the main event). It is necessary to have knowledge about the underlying causes, as well as data and models for determination of the probabilities for different initiating events, for the propagation of outages, and to determine and evaluate the consequences of these cascading outages. Traditional probabilistic methods applied to electric power systems are typically based on normal variations and expectation values and therefore unable to capture extraordinary events with low probability and high impact. In risk analysis it will be necessary to combine power system simulations with expert evaluations to reveal such events. These are problems addressed in ongoing research projects at SINTEF and NTNU.

7 ACKNOWLEDGMENTS

This paper is based on results from the research project Risk and Decision Systems for Critical Infrastructures funded by the Research Council of Norway, and a case study performed in collaboration with the Emergency Preparedness Group of the City of Oslo and the network company Hafslund Nett.

REFERENCES

Billinton, R. & Allan, R. N. 1996. *Reliability evaluation of power systems*, Second Edition. New York, Plenum Press.

Billinton, R., Fotuhi-Firuzabad, M. & Bertling, L. 1999. Bibliography on the application of probability methods in power system reliability evaluation. *IEEE Trans. on Power systems*, Vol. 16, No. 4, Nov. 2001.

Doorman G., Uhlen, K., Kjølle, G. H. & Huse, E. S. 2006. Vulnerability Analysis of the Nordic Power System. *IEEE Trans. on Power Systems*, Vol. 21, No. 1, Febr. 2006.

DSB 1994. *Guidelines for community risk and vulnerability analyses* (in Norwegian: Veileder for kommunale risiko- og sårbarhetsanalyser). Tønsberg: Directorate for Civil Protection and Emergency Planning (DSB).

DSB 2008. *Fire in cable culvert. Oslo Central Station* (in Norwegian: Brann i kabelkulvert. Oslo Sentralstasjon 27.11.2007). Tønsberg: Directorate for Civil Protection and Emergency Planning (DSB).

EPRI 1982. *Transmission system reliability methods, Mathematical models, computing models and results*. EPRI EL-2526, Final Report. New York: PTI

Ericson II., A. C (2005). *Hazard Analysis Techniques for System Safety*. Hoboken: John Wiley & Sons.

EU Commission 2005. On a European Programme for Critical Infrastructure Protection. *Green Paper (COM (2005) 576), Brussels 2005-11-17*

EU Directive 2006. Concerning measures to safeguard security of electricity supply and infrastructure investment. *Directive 2005/89/EC of 18 January 2006*

Kjølle, G., Samdal, K., Singh, B. & Kvitastein, O. 2008. Customer costs related to interruptions and voltage problems: Methodology and results. *IEEE Trans. on Power Systems,* Vol. 23, No. 3, Aug. 2008.

Langset, T., Trengereid, F., Samdal, K. & Heggset, J. 2001. Quality adjusted revenue caps – a model for quality of supply regulation. *In Proc. 2001 International conference & exhibition on electricity distribution.* Amsterdam: CIRED.

NOU 2006. *Official Norwegian Report: When security is the most important* (in Norwegian: Når sikkerheten er viktigst). NOU 2006:6 Oslo: Norwegian CIP Commission

Rausand, M. & Utne, I.B. (2009). *Risikoanalyse. Teori og metoder* (in Norwegian). Trondheim: Tapir Akademisk Forlag

Rinaldi, S. M., Peerenbom J. P., & Kelly T. K. 2001. Identifying, understanding and analyzing critical structures interdependencies. *IEEE Control Systems Magazine,*11-25.

Samdal. K., Kjølle, G. H., Gjerde, O., Heggset, J. & Holen, A. T. 2006. *Requirement specification for reliability analysis in meshed power networks*. Trondheim: SINTEF Energy Research.

Utne, I. B., Hokstad, P., Kjølle, G., Vatn, J., Tøndel, I. A., Bertelsen, D., Fridheim, H. & Røstum, J. 2008. Risk and vulnerability analysis of critical infrastructures – the DECRIS approach. In *SAMRISK conference, Oslo*.

Utne, I. B., Hokstad, P. & Vatn, J. 2009. A structured approach to modeling interdependencies in risk analysis of critical infrastructures. In *ESREL 2009 conference proceedings.* London: Taylor & Francis Group.

Zimmerman, R. 2001. Social Implications of Infrastructure Network Interactions. *Journal of Urban Technology 8*, 97-119.

Zimmerman, R. 2004. Decision-making and the Vulnerability of Interdependent Critical Infrastructure. *IEEE International Conference on Systems, Man and Cybernetics.*