Reliability Engineering and System Safety ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies

G.H. Kjølle [a,*], I.B. Utne [b], O. Gjerde [a]

[a] SINTEF Energy Research, Trondheim, Norway
[b] Department of Marine Technology, Norwegian University of Science and Technology (NTNU), Trondheim, Norway

ARTICLE INFO

Article history:
Received 25 March 2011
Received in revised form
9 January 2012
Accepted 20 February 2012

Keywords:
Critical infrastructures
Risk analysis
Electricity supply
Interdependencies

ABSTRACT

Failures in critical infrastructures can cause major damage to society. Wide-area interruptions (blackouts) in the electricity supply system have severe impacts on societal critical functions and other critical infrastructures, but there is no agreed-upon framework on how to analyze and predict the reliability of electricity supply. Thus, there is a need for an approach to cross-sector risk analyses, which facilitates risk analysis of outages in the electricity supply system and enables investigation of cascading failures and consequences in other infrastructures. This paper presents such an approach, which includes contingency analysis (power flow) and reliability analysis of power systems, as well as use of a cascade diagram for investigating interdependencies. A case study was carried out together with the Emergency Preparedness Group in the city of Oslo, Norway and the network company Hafslund Nett. The case study results highlight the need for cross-sector analyses by showing that the total estimated societal costs are substantially higher when cascading effects and consequences to other infrastructures are taken into account compared to only considering the costs of electricity interruptions as seen by the network company. The approach is a promising starting point for cross-sector risk analysis of electricity supply interruptions and consequences for dependent infrastructures.
© 2012 Elsevier Ltd. All rights reserved.

1. Introduction

Society is critically dependent on a secure electricity supply, and wide-area interruptions (blackouts) have severe impacts on societal critical functions. 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 reliability of electricity supply, even though the power system is defined as one of society's critical infrastructures [1,2]. Critical infrastructures are physical and logical systems with major importance for public welfare. In addition to electricity generation, transmission and distribution, other examples of critical infrastructures are transportation systems, electronic communications, financial services, and water supply [3,4].

There are different kinds of safety and security challenges that critical infrastructures have in common, such as climate changes, natural disasters, ageing of the systems, restructuring of organizations and outsourcing, terrorism, and globalisation (see, e.g., [2]). The infrastructures are also interdependent, because disruptions in one infrastructure may impact the functionality of other infrastructures, for example between electronic communications and the electric power system. The challenges and interdependencies need to be dealt with through in-depth sector studies and interdisciplinary studies across sectors to enable development of methodologies for comparisons and exchange of best practices.

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 cascading failures, for example in other critical infrastructures. In the last two decades, a simple approach to quantitative risk and vulnerability analysis has been applied and adapted separately for different critical infrastructure sectors in Norway [5]. This has resulted in various independent risk assessment approaches, and insufficient analyses of interdependencies between the different sectors. The simplified approach resembles preliminary hazard analysis (PHA) [6].

Various authors analyze and model infrastructure interdependencies (see e.g., [7–17]), and some focus on the electric power system, such as [18–22]. However, since there is no single methodology suitable for risk and vulnerability analysis of extraordinary events in power systems covering all the aspects of causes and consequences, there is a need for combining different quantitative and qualitative methods [23]. The objective of this paper is to provide an approach based on simulations of outages in the electric power system using methods for contingency analysis (power flow) and reliability analysis of power systems. The results

* Corresponding author. Tel.: +4773597275; fax: +4773597250.
E-mail address: gerd.kjolle@sintef.no (G.H. Kjølle).

0951-8320/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2012.02.006

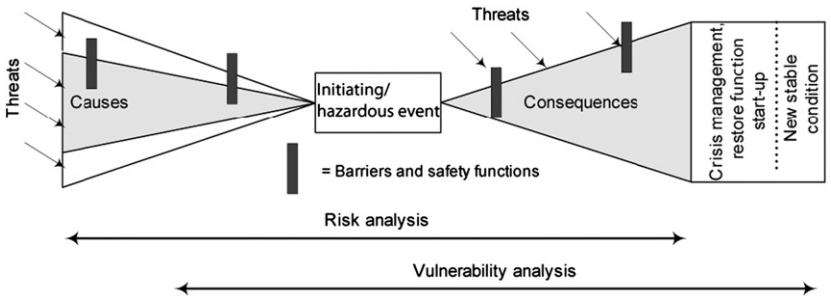

Fig. 1. Bow tie diagram related to risk and vulnerability analysis.

can be used as input, for instance to cascade diagrams [7], in the analysis of the risk of cascading failures and consequences of electricity supply interruptions for other infrastructures.

This paper describes an extension of the simplified approach presented in [24], but expands on the risk analysis of critical infrastructures, emphasizing electricity supply and interdependencies between infrastructures. A case study of the city of Oslo, Norway, was carried out to test and improve the approach in a recent research project[1] which included the critical infrastructures electricity supply, water supply, transport (road/rail), and information and communication systems (ICT). The main focus was on serious events and interdependencies between the sectors. In Norway, the network companies' revenue caps are adjusted in accordance with the customers' interruption costs, CENS [25]. In this arrangement the individual end-user consequences are represented by average cost rates per customer category [26]. CENS represents an estimate of the societal costs of electricity supply interruptions, however only considering the end-user's costs. Consequences when loss of electricity supply results in unavailability of dependent infrastructures, public services etc., are not included in CENS.

The structure of the paper is as follows: First, the cross-sector approach for risk analysis is described with focus on interdependencies between critical infrastructures. Secondly, the approach for risk analysis of electricity supply is presented, as well as the case study. The immediate results are expected number of interruptions of electricity supply, expected interruption duration, interrupted power and energy not supplied for each delivery point. It is shown in a case study that the costs of electricity interruptions for end-users (CENS) might be considerably less than the total costs when cascading effects and consequences to other infrastructures are taken into account.

2. Risk analysis of interdependencies in critical infrastructures

Risk analyses of critical infrastructures across sectors may be far more complicated than traditional analyses, but provide important information for identification of vulnerabilities, emergency preparedness, and prioritization of risk reducing measures. The earthquake in Japan on March 11th 2011, followed by tsunamis and devastation of the coast in the country's north eastern region is a disastrous example of the effect of cascading failures in critical infrastructures: The electricity supply to the cooling systems of some nuclear reactors were destroyed, which led to loss of cooling of the core, subsequent explosions, and leaks of radiation to the environment, as well as threats of nuclear meltdowns [27].

[1] DECRIS – Risk and decision systems for critical infrastructures, http://www.sintef.no/Projectweb/SAMRISK/DECRIS/.

The "bow tie" diagram of Fig. 1 is a useful framework for the risk analysis method described in this paper. The left side of the event represents causes to the hazardous event, and the right side represents the consequences of the event. Based on the consequences, vulnerabilities can be revealed and emergency preparedness planned. Analyses of interdependencies may either focus on the causes, the consequences, or both. In this paper, the consequences of cascading failures are investigated, with the main focus on outages in the electricity supply system.

The approach in this paper consists of five steps, further described in subsequent sections:

1. Plan the analysis
2. Describe initiating event
3. Identify interdependencies
4. Perform risk analysis
5. Risk evaluation.

2.1. Step 1 – Planning

In general, detailed planning of the analysis is necessary to ensure that the risk analysis meets the objectives. If the objectives are not clearly stated irrelevant results may be obtained. The objectives are usually dependent on the stakeholders; i.e., who will make use of the results, and who is affected by them. In risk analyses of critical infrastructures, most often many stakeholders are involved. Thus, identifying stakeholders is part of the initial planning process, along with determining the scope of the analysis and the level of details. Stakeholders may have various motives for carrying out a risk analysis:

- Authorities, such as municipalities and counties, may be concerned about getting a total overview of vulnerabilities and threats within their fields of responsibility. Then they need to assess several sectors as a whole to enable planning of emergency preparedness.
- Owners of the infrastructures, for example of the water supply system or the electricity system, may be more interested in analyses of regularity and system availability.
- Users of the infrastructures, for example large hospitals or transportation companies, may be preoccupied with analyses of own vulnerabilities and dependencies to critical infrastructures, to assess their need for back-up solutions.

Following the definition of objectives and involving relevant stakeholders it is important to determine the scope of the analysis; if it concerns the infrastructures at an overall system level, at subsystem level, or single component level. Other important issues are to determine what kind of consequences should be included, such as service availability, human health issues, human fatalities, damages to assets and the environment; and to what extent the analysis should include malicious acts.

Please cite this article as: Kjølle GH, et al. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. Reliability Engineering and System Safety (2012), doi:10.1016/j.ress.2012.02.006

It is recommended to establish a forum for relevant stakeholders (including system experts) to facilitate exchange of knowledge and discussions about risk perceptions.

2.2. Step 2 – Describe initiating event

The starting point for the risk analysis is the initiating event. This event may already have been identified as an event with high probabilities and/or consequences in previous analyses, and therefore more detailed analysis is needed.

The initiating event description should include physical location, environmental conditions, operating factors, and assessments to whether there is a gross accident potential, if there are communication challenges to the public, and how the initiating event may impact physical objects in close proximity [7].

An important issue is to determine the societal critical functions (SCFs) affected. SCF is a term used to represent critical functions, and a particular infrastructure may have one or more SCFs [7]. The SCFs affected by the event should be investigated in terms of if they were a cause to the initiating event, or if they were impacted by the initiating event itself, immediately or with some time delay.

2.3. Step 3 – Identify interdependencies

The next step of the risk analysis should be to identify interdependencies of which there are different types. In [28] it is distinguished between *spatial* and *functional* interconnectedness and dependency. Spatial interconnectedness refers to proximity between infrastructures as the most important relationship between the systems. Functional interconnectedness refers to a situation in which an infrastructure is necessary for operation of another infrastructure, for example, the pumps in a water treatment system needing electricity in order to function. This paper focuses on location-specific (physical) interdependencies and functional interdependencies, corresponding to the above-mentioned categories. Interdependencies and barriers should be considered with respect to all causes of the initiating event (including security issues, for example, to prevent malicious acts), as well as redundancy. A procedure for revealing interdependencies is thoroughly explained in [7].

To visualize, analyze, and communicate the interdependencies between stakeholders, a cascade diagram may be used, such as the example in Fig. 7 in Section 4. A cascade diagram gives an overview of interdependencies in a structured manner and resembles an event tree, but focuses on consequences in terms of interdependencies. The cascade diagram is constructed by placing the initiating event to the left in the diagram. Thereafter, all affected location-specific SCFs are placed to the right and connected with lines to the initiating event. The SCFs related to the functional interdependencies are then introduced in the rightmost part. As interdependencies further out in the chain of cascading events are revealed, the cascade diagram is expanded. The SCFs to the very right in the diagram are called leaf nodes, i.e., those interdependencies for which further analysis is found unnecessary.

The cascade diagram may be used as basis for qualitative or quantitative risk analysis of interdependencies.

2.4. Step 4 – Perform risk analysis

A qualitative analysis of the cascade diagram is beneficial if there are limited resources available and the stakeholders are not familiar with risk modeling. However, often a qualitative analysis will be too coarse, and some kind of quantification is needed. An approach to a semi-quantitative analysis of the cascade diagram and calculations of risk are proposed in [7].

If more specific information is needed about an infrastructure or interdependency, detailed quantitative analyses may be carried out, such as the analysis presented in Section 3 for electricity supply.

2.5. Step 5 – Risk evaluation

This step includes documentation and evaluation of risk reducing measures. The results from the detailed analyses have to be integrated into the risk analysis, and possible risk-reducing measures evaluated. It is necessary to assess whether the accident scenario may occur under similar circumstances in other locations, if the accident scenario has higher or lower risks than similar scenarios and systems, and whether further analyses are needed. Critical junctions and weak barriers should also be evaluated.

Risk reducing measures may be suggested based on the cascade diagram, and their effect on the risk investigated [7]. In general, an overall list of suggested risk reducing measures should be provided, for example related to interdependencies that have to be reduced by different types of physical separation or by redundancy. The assessments of risk reducing measures should be carried out in cooperation with the stakeholders, and may also imply more formal trade-offs in terms of a cost/benefit-analysis. An approach to cost/benefit analysis related to risks of interdependencies is suggested in [7].

3. Risk analysis of electricity supply

The electricity system is an extremely complex and comprehensive infrastructure. Despite the numerous components and the complexity of the system it 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 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,[2] local networks are mostly operated as radials and any component outage due to a failure will lead to interruption of electricity supply.

Hazardous 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. 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 (physical) dependencies, for instance two power lines on the same tower or in the same right-of-way, or 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.

As far as the electricity system is concerned, probabilistic approaches to reliability evaluation are rather mature, see, e.g., [29,30]. Generally, these approaches aim to measure the capability of the system to supply the load in the steady state (adequacy)

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

Please cite this article as: Kjølle GH, et al. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. Reliability Engineering and System Safety (2012), doi:10.1016/j.ress.2012.02.006

in which the power system may exist considering normal conditions. There is no established framework on how to analyse and predict the security (reliability) of electricity supply, meaning the ability of an electricity system to supply final customers with electricity [31], 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 impacts on society [32]. Case studies and experiences so far indicate that one of the most challenging parts of a risk and vulnerability analysis of electric power systems is to identify vulnerable operating states and extraordinary events that could lead to wide area interruptions and to further identify the consequences of these events [23].

Consequences of power system failures can, for instance, be classified according to the amount of disconnected load and stipulated average (weighted) duration. Fig. 2 gives an example of a consequence diagram using these two dimensions for some blackouts in the past [30,31]. The figure also shows the classification of consequences from minor to catastrophic [30]. This classification depends upon the system or area under study. There are two groups of events shown in Fig. 2. Events in the first group to the left are typically initiated by technical or operational failures causing interruptions of limited duration but varying size in terms of area and load affected. The worst event (in terms of disconnected load) in the first group is the blackout of major parts of Europe in November 2006 (“Europe, UCTE 2006”). The second group to the right consists of events where natural hazards (wind, icing) have caused wide area damages to power lines resulting in comprehensive repair and extremely long durations. In this group the Canadian ice-storm in 1998 (“Canada 1998”) caused the most severe consequences in terms of disconnected load and stipulated average duration.

Fig. 3 gives an example of a risk graph, showing only the hazardous events from Fig. 2 where probability information is available [32]. Here consequences in terms of energy not supplied, provided by disconnected load and stipulated duration from Fig. 2, are plotted against expected frequency to occur. The figure shows that even though two of the events, “Sweden 1983” and “Southern Sweden/Eastern Denmark 2003”, give critical consequences (Fig. 2) the risk is moderate due to the expected infrequent occurrence (low probability).

Previous studies indicate that there is no single methodology suitable for risk and vulnerability analysis of extraordinary events in power systems covering all the aspects of causes and consequences [23]. There is a need for combining different quantitative and qualitative methods. Examples of methods regarded as the most relevant and supporting the different aspects are described in [23]. Among the relevant quantitative methods are contingency analysis and power flow analysis [29,30,41]. These analyses constitute the basis for reliability analysis of power systems, and may be supported by fault and event trees (for details about these methods, see, e.g., [34]), as well as expert evaluations and various other qualitative methods.

For the detailed risk analysis (step 4 in Section 2) and case study presented in this paper, it was chosen to utilize the well-established methodology for reliability analysis of electric power systems, denoted the contingency enumeration approach [37,41]. In a cross-sector risk analysis, where the initiating event occurs in the electricity supply system, the contingency enumeration approach constitutes the basis for describing the initiating event before moving on to investigation of interdependencies to other critical infrastructures.

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 initiating event “loss of electricity supply to a delivery point”. The contingency enumeration approach comprises three main steps:

A. Selection and evaluation of contingencies
B. Consequence analysis of contingencies
C. Reliability assessment and accumulation of reliability indices.

Step A of the contingency enumeration approach aims at reducing 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 step B the delivery points that will experience interruptions (or reduced supply) are identified. This analysis of electrical

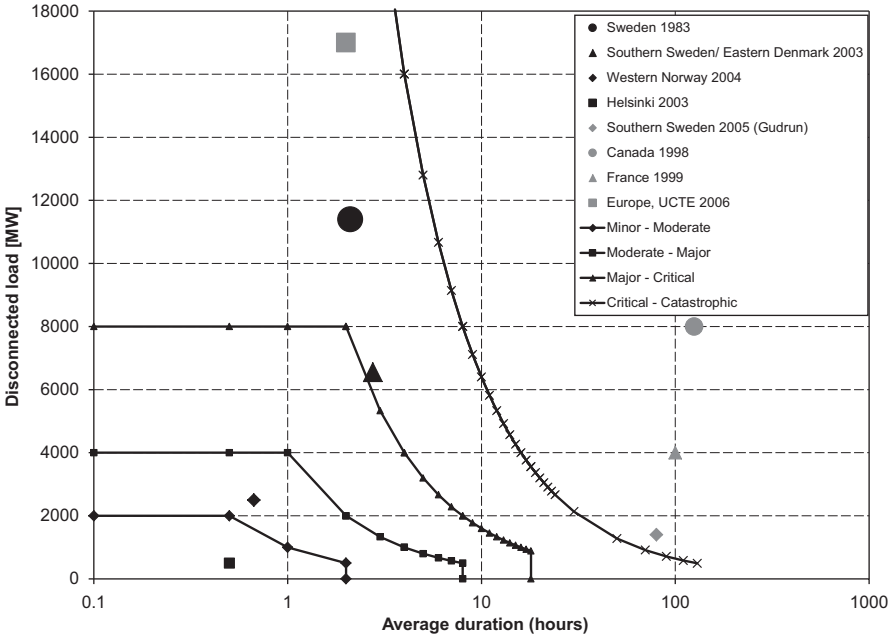

Fig. 2. Consequence diagram for the electricity supply, based on [32,33].

Please cite this article as: Kjølle GH, et al. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. Reliability Engineering and System Safety (2012), doi:10.1016/j.ress.2012.02.006

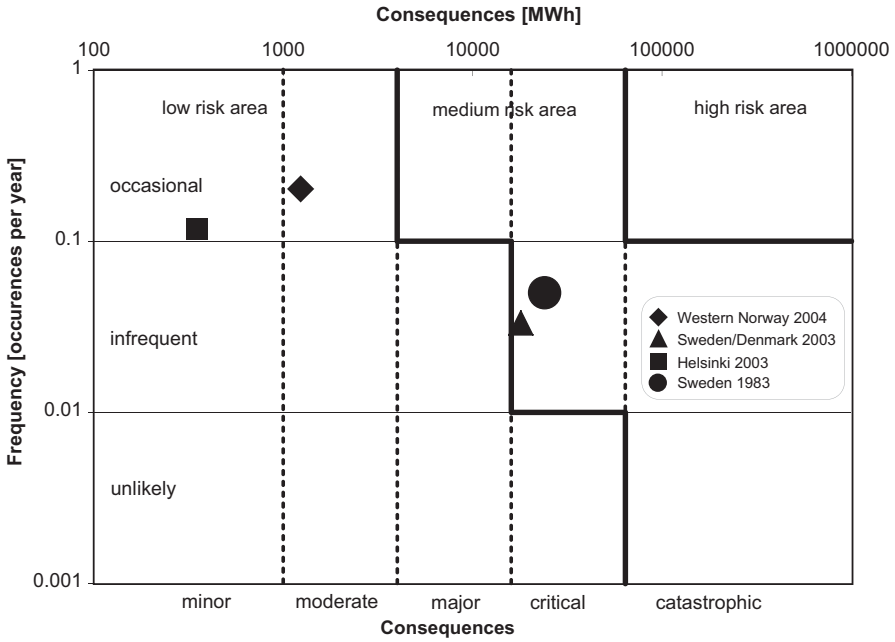

Fig. 3. Risk graph, based on [32].

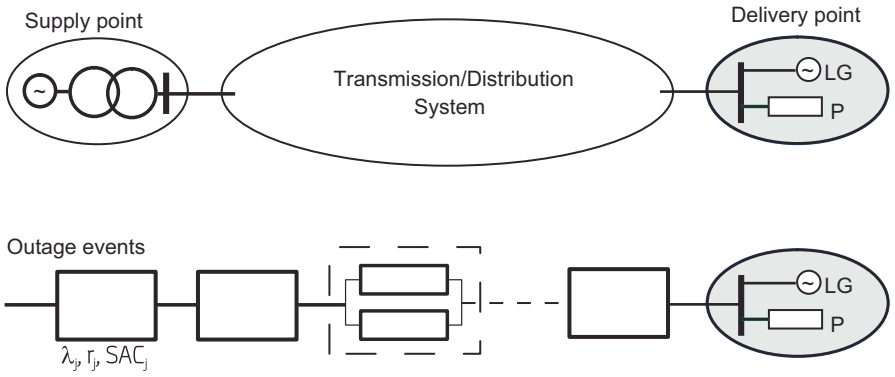

Fig. 4. Reliability model for a general delivery point based on minimal cut sets [38,39].

consequences is based on simulations of contingencies in the electric power system using physical power flow models [23,39,41]. The final step C 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 Fig. 4, describing a minimal cut set structure for the electricity supply to the 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

The reliability assessment (step C) uses the model in Fig. 4 taking the critical contingencies (outage events) for a delivery point as a starting point. These contingencies are those found to cause problems through the identification and analysis of contingencies in step A and B, constituting the minimal cut sets for the delivery point). 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. The electricity supply to a certain delivery point is interrupted when the available power capacity after the occurrence of a given contingency is unable to match the load, i.e., when $P > SAC+LG$. The equivalent failure rates and outage times are determined using basic frequency and duration techniques for parallel systems, while the total frequency and duration of interruptions are found by accumulation of the contributions from the minimal cut sets using the basic techniques for series systems (cf. Fig. 4) as described in, e.g., [29]. The method combining contingency and reliability analysis is described in detail in [38].

The contingency enumeration approach is used for at least one operating 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 power exchange with neighbouring areas. This approach requires various types of data about the power system under study, such as components, loads and end-users, data from failure statistics, operating procedures, and reserve supply possibilities.

Please cite this article as: Kjølle GH, et al. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. Reliability Engineering and System Safety (2012), doi:10.1016/j.ress.2012.02.006

The basic delivery point reliability indices are expected number of interruptions of electricity supply and expected interruption duration, while the consequences are the disconnected load and energy not supplied. The expected duration and amount of disconnected load describe the severity in case of electricity supply interruptions to the delivery point (cf. Fig. 2).

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 approach presented in this section addresses all these parts for the electricity supply to a delivery point. 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 the expected number of interruptions and energy not supplied can be regarded as risk indices. The next section exemplifies the approach.

4. Case study – Loss of electricity supply

A case study according to steps 1–5 described in Section 2, was carried out in collaboration with the Emergency Preparedness Group (EPG) of the city of Oslo. Previous risk and vulnerability analyses of Oslo [35,36] were used as a basis for the case study which involved serious events in several infrastructures, covering events of technical character, malicious acts, as well as natural hazards. One of the events subject to detailed analysis was "loss of electricity supply to Oslo central station (Oslo S)". The analyses, carried out in collaboration also with the network company Hafslund Nett, are shown step by step in the following. The main focus is on the detailed quantitative analyses of step 4.

4.1. Step 1 – Planning

The stakeholders in this case study are represented by the EPG and Hafslund nett. EPG is an organization working with safety and cooperation between the critical infrastructure owners of water supply, electricity supply, ICT, hospital, harbor, transportation, and fire and rescue services in the municipality.

The scope of the analysis concerns the infrastructures at an overall system level, and consequences include service availability for the electric power system and connected infrastructures calculated as monetary values.

4.2. Step 2 – Describe initiating event

The initiating event was "loss of electricity supply to Oslo S". Oslo S is the main railway station where numerous service providers and users are located, of which some represent critical infrastructures and societal critical functions, in addition to shops, etc.

Fig. 5 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 distribution network mainly consists of 11 kV underground cables.

According to the network company's interruption statistics for the period 2001–2007, the end-users of Hafslund Nett will experience an interruption on average every second year with an expected duration of 18 min per interruption due to failures in the regional network (down to level 2 in Fig. 5). Including failures in the distribution network (levels 3 and 4 in Fig. 5) the number of interruptions increases to 0.8 per year with an expected annual duration of 40 min. Thus, the regional network contributes to about 60% of the number of interruptions, while the distribution network stands for 67% 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 electricity end-users. Both these events lasted for less than one hour. The third event, at Oslo S in 2007 [40], started as a minor fire in an 11 kV cable in the distribution network, caused by digging in the area around the central station. The fire led to evacuation of the station. Several communication systems were interrupted, including train operation services, internet and phone services. It took 16 h before the electricity supply was restored and another 4–5 h before the central station was reopened for the public and the train traffic resumed [40]. For visualization these three hazardous events are plotted in the consequence diagram in Fig. 6. This diagram is similar to Fig. 2, but it can be noted that the consequence classes in Fig. 6 are scaled to fit the size of the power system in Oslo and to provide an illustration of the degree of criticality of events. This is not an official classification used by the network company.

As can be seen from the Fig. 6 the two 300 kV events (in the main grid, cf. Fig. 5) were large in terms of disconnected load, but caused relatively short interruption duration and thus limited consequences for infrastructures. The event at Oslo S caused low disconnected load, but considerably longer duration of the loss of electricity supply to the central station. The three events can, according to Fig. 6, be considered from major to critical. However, the Oslo S event (11 kV distribution system) was very different from the two events in the main grid (300 kV). Even so, they are all examples of different events leading to the initiating event "loss of electricity supply to Oslo S".

4.3. Step 3 – Identify interdependencies

The event at Oslo S was selected because there are other infrastructures present that to a large extent depend on electricity supply. In a cross-sector risk analysis it is necessary to identify interdependencies between infrastructures and consequences for these infrastructures if the electricity supply is interrupted.

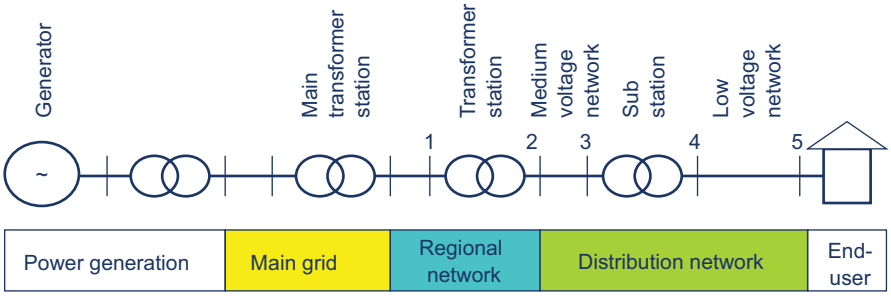

Fig. 5. Stylized overview of the power system (value chain) from power generation to demand, source: Hafslund Nett.

Please cite this article as: Kjølle GH, et al. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. Reliability Engineering and System Safety (2012), doi:10.1016/j.ress.2012.02.006

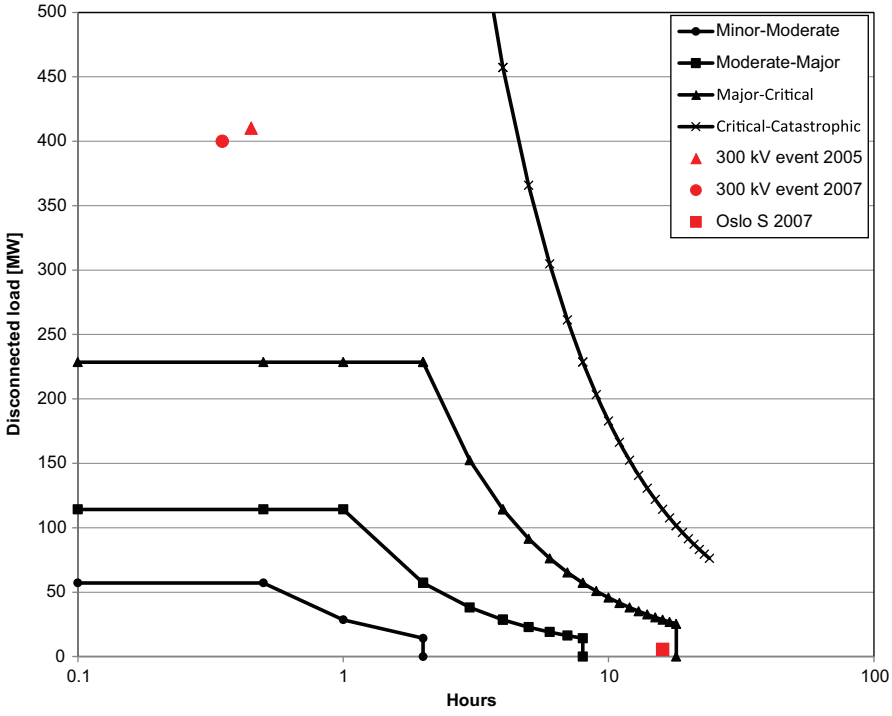

Fig. 6. Hazardous events in the electric power system in Oslo.

It is a challenge for network companies to have detailed knowledge about the different end-users behind each delivery point. Consequences of electricity supply interruptions to other infrastructures need to be investigated by focusing on interdependencies, involving the stakeholders being responsible for the operation of the infrastructures.

The initiating event "loss of electricity supply to Oslo central station (Oslo S)" may, as was shown above, be caused by outage of transformer stations, power lines or cables in the main grid and regional network in Oslo (Fig. 5). The event is critical if it occurs in heavy load situations, usually in cold winter periods. In such situations the reserve electricity capacity is limited. Electricity supply interruptions may also be critical to dependent infrastructures, such as railway transportation and banking services.

The simplified cascade diagram in Fig. 7 shows the interdependencies between electricity supply and other critical infrastructures, like the major railway station in Oslo (Oslo S). A general loss of electricity supply to the railway station will mainly cause consequences due to functional interdependencies, shown in the cascade diagram.

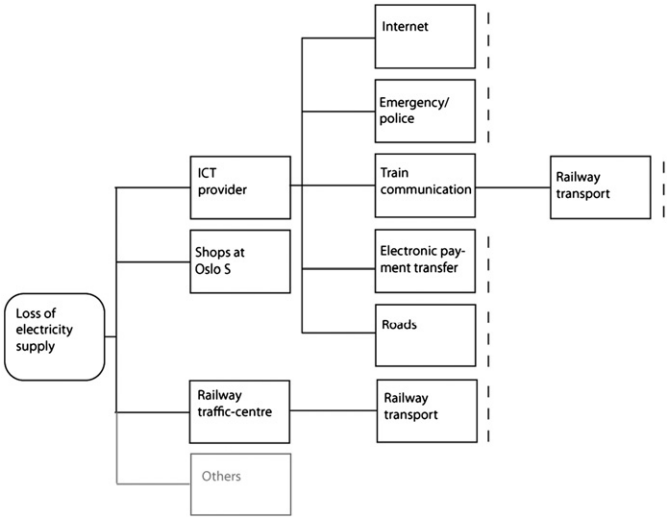

Fig. 7. Simplified cascade diagram for loss of electricity supply for the Oslo central station, based on [7]. The dashed lines indicate leaf-nodes.

4.4. Step 4 – Perform risk analysis

A reliability analysis of the power system of Oslo was carried out according to the contingency enumeration approach described in Section 3 (steps A–C). It was used to estimate how often an initiating event will occur (number and duration of electricity supply interruptions to different delivery points) and the consequences in terms of interruption duration, the amount of interrupted load, energy not supplied (ENS) and the corresponding cost (CENS).

Table 1 shows the result of the analysis for the heavy load situation for two different transformer stations in the 33 kV network in the inner parts of Oslo. For Station A, which has the highest expected interruption frequency, the minimal cut sets include single outages of five power transformers and four cables, as well as a common mode failure of cables in the same culvert.

Table 1
Reliability indices for 33 kV delivery points. Including single line and transformer outages and common mode. (Reconnection possibilities not included).

Delivery point	Number of interruptions	Duration	Energy not supplied (ENS)
	(per year)	(h)	(MW h/year)
Station A	3.0	71	2340
Station B	0.12	371	292

The minimal cuts for Station B consist of three single cable outages and common mode failure of cables underneath a road bridge (location-specific interdependency). Oslo S is supplied

Please cite this article as: Kjølle GH, et al. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. Reliability Engineering and System Safety (2012), doi:10.1016/j.ress.2012.02.006

ARTICLE IN PRESS

from Station B and loss of electricity supply can be expected once every 8 years (expectation value of 0.12 interruptions/year).

In the case presented in Table 1, reserve connection possibilities are not considered. 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. For instance it will take about 1 h 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. As an example, it may take 4–24 h to connect reserve supply from underlying distribution network and up to four 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 [38].

Keeping in mind the assumptions and premises for the analysis described above, the results presented in Table 1 are not realistic for the actual electricity supply to Oslo S. 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.

As mentioned Oslo S is supplied from Station B while Station A serves some other 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. Since the results in Table 1 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 Table are given in units per year as if the heavy load situation lasts for the whole year. One should keep in mind that the heavy load situation is regarded as worst case, but this situation only lasts for a small portion of the year. However, for the emergency preparedness of other critical infrastructures it is important to consider the worst case outcome of interrupted electricity supply.

The consequences of the initiating event may be found when analysing interdependencies and developing the cascade diagram. Table 2 illustrates the consequences of the actual event when Oslo S lost the electricity supply in 2007 (Fig. 6), due to fire in a cable culvert [40].

The event started in the electric power system, but caused rather limited consequences in the power system in terms of disconnected load (cf Fig. 6). Even if the electricity supply interruption lasted for 16 h the CENS cost was calculated to approx. 4.5 MNOK only. CENS is calculated as the product of ENS (in kW h) and a cost rate in NOK/kW h for different customer groups [25,26]. In this case ENS = 42.5 MW h and the average cost rate about 105 NOK/kW h. This cost is seen by the network company. In railway transportation a delay is often valued in the range of 3 NOK per passenger minutes lost [7]. Assuming that all the 80 000 passengers were delayed for 20 h, this results in a societal cost of passenger minutes lost of approximately 300 MNOK, which is nearly seventy times higher than the CENS cost. In addition, there are societal costs related to the loss of internet services for 25 000 users for 10 h, as well as other direct and indirect consequences, such as increased road traffic, closed shops, etc.

Table 2
Cross infrastructure consequences of loss of electricity supply to Oslo railway station [40].

Infrastructure	Consequence
Electricity supply	Loss of 5.6 MW load, interruption duration 16 h, CENS = 4.5 MNOK
Railway transport	80 000 passengers delayed for 20 h, cost ≈ 300 MNOK (see below)
Internet	25 000 users without services for 10 h
Traffic control centre	Loss of control centre for some (unspecified) time

The different estimations in costs visualize the challenges in cost-benefit analysis when risk assessments only deal with one infrastructure, and demonstrate the importance of a cross-sector approach.

4.5. Step 5 – Risk evaluation

The risk analysis of the electricity supply and the further investigation of interdependencies and consequences for other critical infrastructures can be used to assess the need for risk reducing measures, for example in the electricity supply system itself or with respect to back-up solutions or redundancy in other infrastructures (e.g., the railway traffic centre at Oslo S in Fig. 7).

This part was not further pursued as risk evaluation was not a part of this case study. The main goal was rather to develop and test methodology for cross sector risk analyses, and show how important results can be obtained as a basis for further work including risk evaluation.

5. Discussion and conclusions

This paper presents a cross-sector approach for risk analysis of critical infrastructures emphasizing electricity supply and interdependencies between infrastructures. A case study of the city of Oslo was carried out to test and improve the method in a recent research project comprising electricity supply, water supply, transport (road/rail), and information and communication systems. Analyses of interdependencies may either focus on the causes, the consequences, or both. In this paper, the consequences of cascading failures are investigated, mainly focusing on the electricity supply.

There is no single methodology available for risk and vulnerability analyses of hazardous (extraordinary) events in the electric power system, and there is a need for combining different qualitative and quantitative methods. In this paper, the contingency enumeration approach is used to simulate the electrical consequences of outages in the power system and to estimate how often electricity supply will be interrupted to specific delivery points, as well as the duration of these outages. This is important information that enables further identification of interdependencies to be used in a cascade diagram. The cascade diagram can provide an overview of interdependences to other infrastructures and, as such, is a means for investigating and analysing consequences in other infrastructures, providing a basis for risk assessment and emergency preparedness planning. The approach described in this paper may also give information about the area affected, disconnected load, energy not supplied and corresponding societal costs.

In a cross-sector risk analysis it is important to gather sufficient competence and information from the stakeholders involved. The case study provided valuable opportunities for improved communication between stakeholders and infrastructure owners in the Emergency Preparedness Group of Oslo. The results highlight the need for cross-sector analyses and show that the approach presented in this paper is a promising basis for risk analysis of wide-area interruptions of electricity supply and the

Please cite this article as: Kjølle GH, et al. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. Reliability Engineering and System Safety (2012), doi:10.1016/j.ress.2012.02.006

ARTICLE IN PRESS

consequences for other critical infrastructures through cascade diagrams.

The consequences due to loss of electricity supply incur different costs, depending on which stakeholder is affected. The CENS cost (which is the cost for the network company due to loss of electricity supply to delivery points) is in this case significantly lower than the costs for society due to loss of railway transportation. When evaluating risk and determining the needs for risk reduction, such differences may have substantial impact on cost-benefit analysis and implementation of risk reducing measures. When just focusing on CENS cost the incentives for implementing risk reducing measures in dependent infrastructures are much lower than if interdependencies are modelled and costs are calculated in a wider context, including consequences to dependent critical infrastructures. Thus, the case study results have highlighted the need for cross-sector analyses. The approach presented in this paper is a promising starting point for a cross-sector risk analysis where the initiating event occurs in the electric power system.

In detailed risk analysis of electricity systems, a major challenge is to identify chains of events that could lead to wide-area interruptions. Contingencies leading to severe consequences will most likely be caused by extraordinary events composed by, e.g., two or more failures in the main grid, malfunctioning of the protection system, or grid failure when one or more large power plants are on outage. It is necessary to have knowledge about the underlying causes, as well as data and models for determining the probabilities for different initiating events, for the propagation of outages, and to be able to identify and evaluate the consequences of cascading failures. Such multiple events are regarded to have low probability. Traditional probabilistic methods applied to electric power systems are typically based on normal variations and expectation values and are therefore not well suited to capture extraordinary events with low probability and high impact. Further work is also needed to identify the consequences of interrupted electricity supply to infrastructures, such as transport, water supply and telecommunication. Examples are problems for traction power supply, tunnel lighting, pumping systems, and base stations for mobile phone systems. These challenges are addressed in ongoing research projects at SINTEF and NTNU.

Acknowledgments

This paper is based on results from the recent research project Risk and Decision Systems for Critical Infrastructures (DECRIS) 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. We greatly acknowledge all the partners in DECRIS and all stakeholders involved in the case study.

References

[1] EU Commission. On a European Programme for Critical Infrastructure Protection. Green Paper (COM (2005) 576), Brussels 2005;11–17.
[2] NOU. Official Norwegian Report: When security is the most important (in Norwegian: Når sikkerheten er viktigst). NOU 2006:6 Oslo: Norwegian CIP Commission.
[3] Abou El Kalam A, Deswarte Y, Baïna A, Kaâniche M. PolyOrBAC: a security framework for critical infrastructures. International Journal of Critical Infrastructure Protection 2009:154–69.
[4] Rinaldi SM, Peerenboom JP, Kelly TK. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine 2001:11–25.
[5] DSB. Guidelines for Community Risk and Vulnerability Analyses (in Norwegian: Veileder for kommunale risiko- og sårbarhetsanalyser). Tønsberg: Directorate for Civil Protection and Emergency Planning (DSB); 1994.
[6] Ericson II CA. Hazard Analysis Techniques for System safety. John Wiley & Sons; 2005.
[7] Utne IB, Hokstad P, Vatn J. A method for risk modeling of interdependencies in critical infrastructures. Reliability Engineering & System Safety 2011; 96(6):671–8.
[8] Rinaldi S Modeling and simulating critical infrastructures and their interdependencies. 37th Hawaii International Conference on System Sciences; 2004.
[9] Haimes Y, Horowitz B, Lambert J, Santos J, Lian C, Crowther KG. Interoperability input–output model for interdependent infrastructure sectors. I: Theory and methodology. Journal of Infrastructure Systems 2005;11(2): 67–79.
[10] Haimes Y, Horowitz B, Lambert J, Santos J, Lian C, Crowther KG. Interoperability input–output model for interdependent infrastructure sectors. II: Case studies. Journal of Infrastructure Systems 2005;11(2):80–92.
[11] Pederson P, Dudenhoeffer D, Hartley S, Permann M Critical Infrastructure Interdependency Modeling: A Survey of US and International Research Technical Report. Idaho National Laboratory, INL/EXT-06-11464; 2006.
[12] Lian C, Haimes Y. Managing the risk of terrorism to interdependent systems through the dynamic interoperability input–output model. Systems Engineering 2006;9(3):241–58.
[13] Min HSJ, Beyeler W, Brown T, Son YJ, Jones AT. Toward modeling and simulation of critical national infrastructure interdependencies. IIE Transactions 2007;39(1):57–71.
[14] Rahman HA, Beznosov K, Marti JR. Identification of sources of failures and their propagation in critical infrastructures from 12 years of public failure reports. International Journal of Critical Infrastructures 2009;5(3):220–44.
[15] Myers JD, Sorrentino jr MA. Regional critical infrastructure assessment: Kansas City. International Journal of Critical Infrastructures 2011;7(1):58–72.
[16] Zio E, Piccinelli R, Sansavini G. An all-hazard approach for the vulnerability analysis of critical infrastructures. In: Berenguer, Grall, Soares Guedes, editors. Advances in Safety, Reliability and Risk Management. London: Tayor & Francis Group; 2012.
[17] Nan C, Kröger W, Probst P. Exploring critical infrastructure interdependency by hybrid simulation approach. In: Berenguer, Grall, Soares Guedes, editors. Advances in Safety, Reliability and Risk Management. London: Tayor & Francis Group; 2012.
[18] Kroger W. Critical infrastructures at risk: securing electric power supply. International Journal of Critical Infrastructures 2006;2:273–93.
[19] Shih CY, Scown CD, Soibelman L, Matthews HS, Garret Jr J, Dodrill K, et al. Data management for geospatial vulnerability assessment of interdependencies in U.S. power generation. Journal of Infrastructure Systems 2009;15(3): 179–89.
[20] Johansson J Risk and vulnerability analysis of interdependent technical infrastructures. Addressing socio-technical systems. Doctoral Thesis in Industrial Automation. Department of Measurement Technology and Industrial Electrical Engineering, Lund University; 2010.
[21] Rigole T, Vanthournout K, De Brabandere K, Deconinck G. Agents controlling the electric power infrastructure. International Journal of Critical Infrastructures 2008;4:96–109.
[22] Volkanovski A, Cepin M, Mavko B. Application of the fault tree analysis for assessment of power system reliability. Reliability Engineering & System Safety 2009;94(6):1116–27.
[23] Gjerde O, Kjølle GH, Detlefsen NK, Brønmo G. Risk and vulnerability analysis of power systems including extraordinary events. IEEE PES Trondheim Powertech 2011.
[24] Kjølle G, Utne IB. Critical Infrastructures and Risk Analysis of Electricity Supply. London: Taylor & Francis Group; 2010.
[25] Langset T, Trengereid F, Samdal K, Heggset J Quality adjusted revenue caps – a model for quality of supply regulation. International Conference and Exhibition on Electricity Distribution. Amsterdam: CIRED; 2001.
[26] Kjølle G, Samdal K, Singh B, Kvitastein O. Customer costs related to interruptions and voltage problems: methodology and results. IEEE Transactions on Power Systems 2008;23(3):1030–8.
[27] Tabuchi H, Wald ML. Partial meltdowns presumed at crippled reactors. New York Times 2011. http://www.nytimes.com/2011/03/14/world/asia/14nuclear.html?_r=1&hp.
[28] Zimmerman R. Social implications of infrastructure network interactions. Journal of Urban Technology 2001;8:97–119.
[29] Billinton R, Allan RN. Reliability Evaluation of Power Systems.2nd edn. New York: Plenum Press; 1996.
[30] Billinton R, Fotuhi-Firuzabad M, Bertling L. Bibliography on the application of probability methods in power system reliability evaluation 1996–1999. Power Engineering Review, IEEE 2001;21(8):56.
[31] EU Directive. Concerning measures to safeguard security of electricity supply and infrastructure investment. Directive 2005/89/EC of 18 January 2006.
[32] Doorman G, Uhlen K, Kjølle GH, Huse ES. Vulnerability analysis of the Nordic power system. IEEE Transactions on Power Systems 2006;21(1):402–10.
[33] NordSecurEl. Risk and vulnerability assessments for contingency planning and training in the Nordic electricity system. Final report, Statens Energimyndighet, EU EPCIP, Eskilstuna; 2009.
[34] Rausand M, Høyland A. System Reliability Theory. Models, Statistical Methods and Applications. Hobroken, NJ: Wiley; 2004.
[35] Sklet S, Tinmannsvik RK, Øien K Safety and emergency preparedness in Oslo municipality (In Norwgian: Sikkerhet og beredskap i Oslo kommune). Restricted Report. Trondheim, Norway: SINTEF Safety and Reliability; 1997.

Please cite this article as: Kjølle GH, et al. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. Reliability Engineering and System Safety (2012), doi:10.1016/j.ress.2012.02.006

ARTICLE IN PRESS

[36] SAFETEC. Oslo municipality, Emergency Planning Agency, Main report, Update of RVA analysis (In Norwegian: Oslo kommune, Beredskapsetaten, Hovedrapport- Oppdatering av ROS-analyse). Restricted Report; 2004.
[37] EPRI. Transmission system reliability methods, Mathematical models, computing models and results. EPRI EL-2526, Final Report. New York: PTI; 1982.
[38] Samdal K, Kjølle GH, Gjerde O, Heggset J, Holen AT. Requirement Specification for Reliability Analysis in Meshed Power Networks. SINTEF Energy Research, Trondheim 2006.
[39] Kjølle G, Gjerde O. Integrated approach for security of electricity supply analysis. International Journal of Systems Assurance Engineering and Management 2010;1(2):163–9.
[40] DSB. 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); 2007.
[41] Billinton, R. Composite system adequacy assessment – the contingency enumeration approach, IEEE Tutorial Course Reliability assessment of composite generation and transmission systems, course text 90EH0311-1-PWR, 1989, Paper no 5.

Please cite this article as: Kjølle GH, et al. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. Reliability Engineering and System Safety (2012), doi:10.1016/j.ress.2012.02.006