Risk and Vulnerability Analysis of Power Systems Including Extraordinary Events

Oddbjørn Gjerde, Gerd H. Kjølle, *Member, IEEE*, Nina K. Detlefsen and Geir Brønmo

***Abstract*—This paper describes a framework and methodology for risk and vulnerability analysis including extraordinary events in power systems. The framework is based on a bow-tie structure and identifies threats, unwanted events, barriers and consequences. Application of the methodology is shown for a real case analyzing extraordinary events in a transmission system. In this case the consequence is unacceptable, but the risk is moderate due to the low probability for the event to occur. The case study and experience so far indicates that one of the most challenging parts of a risk and vulnerability analysis is how to identify the vulnerable operational states and extraordinary events.**

***Index Terms*—Power systems, risk and vulnerability, extraordinary events, barriers, causes, consequences.**

I. Introduction and Background

ALTHOUGH the power system at transmission level usually is dimensioned and operated according to the N-1 criterion, history shows that blackouts still occur in different parts of the world [1]. Such wide-area interruptions in the electricity supply have severe impacts on society's critical functions, and there is a need for tools and methods to structure and analyze events, causes and consequences.

The study of power system reliability has long traditions. Relevant literature is often concerned with either generation adequacy or system security, e.g. [2, 3]. Classical contingency analyses are based on expectation values and usually consider only a few operational states like e.g. heavy and light load. With such an approach it may be difficult to reveal special combinations of events leading to large consequences, but with low probability (extraordinary events, or high impact low probability events). More recently several papers are addressing power system vulnerability [4, 5]. In [6] a methodology is presented where the three different types of incidents; energy shortage, capacity shortage, and power system failures, are presented in one unified framework.

The methodology presented in this paper is based on the approaches from [6] and [7] describing a framework for power system risk and vulnerability analysis. This framework is under development in an ongoing research project and is demonstrated on a real case in the paper.

II. Methodology for Risk and Vulnerability Analysis

A. Framework for extraordinary events

The framework uses the bow tie-model as a starting point to describe the relations between main causes and consequences of an unwanted event [8]. An example is given in Figure 1 below. The main unwanted events to be considered here are power system failures and the consequences in terms of wide-area interruptions or blackouts. This is shown in the figure together with major categories of threats including natural hazard (e.g. a major storm), technical/operational causes, human errors and antagonistic causes such as terror or sabotage.

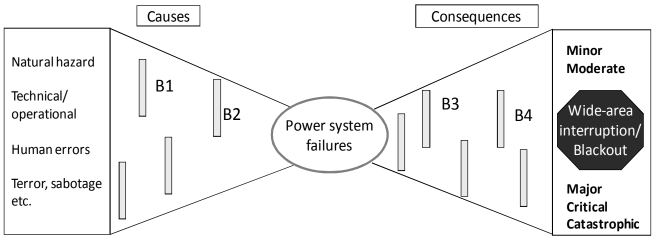

Fig. 1. Threats, unwanted (extraordinary) event, consequences and barriers

The threats might lead to power system failures through a chain of events and a set of causes, while the failure(s) might lead to minor or severe consequences through a set of circumstances.

As indicated in the figure, a number of barriers exist to avoid threats to develop into unwanted events and to prevent or reduce the consequences. A system is more vulnerable towards the relevant threats if the barriers are weak or malfunctioning.

In risk and vulnerability analysis of electric power systems a major challenge is to identify chains of events that could lead to wide-area interruptions. It is necessary to have knowledge about the underlying causes, and to determine and evaluate the consequences of these events.

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 the two dimensions disconnected load and average duration for some blackouts in the past [6, 7].

O. Gjerde and G. H. Kjølle are with SINTEF Energy Research, N-7465 Trondheim, Norway (e-mail: Oddbjorn.Gjerde@sintef.no; Gerd.Kjolle@sintef.no).

N. Detlefsen and G. Brønmo are with Energinet.dk, DK-7000 Fredericia, Denmark (e-mail: nid@energinet.dk; geb@energinet.dk)

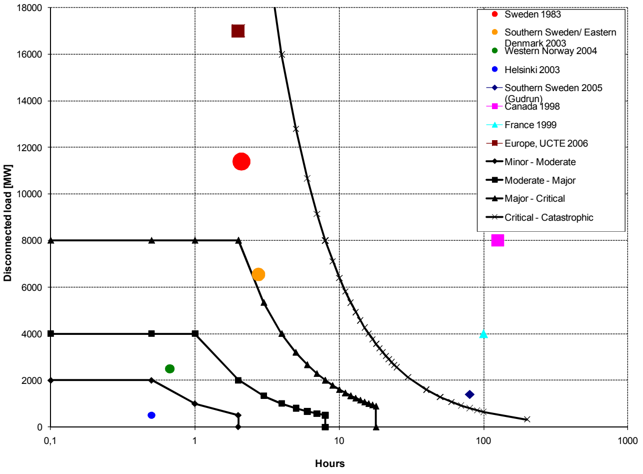

Fig. 2. Consequence diagram [6, 7]

Risk is defined as a combination of the probability of an event to occur, and its consequence. For some unwanted events it might be feasible to estimate the probability of occurrence, and further the risk. Fig. 3 gives an example of a risk diagram where risk is plotted for the unwanted events in Fig. 2 where probability information is available. The figure shows that even though two of the events give critical consequences the risk is moderate due to the infrequent occurrence (low probability). Working with high impact, low probability (HILP) events risk diagrams are not always appropriate as the consequence might still be unacceptable even if the risk is medium/low. Supplementing evaluations may therefore be necessary.

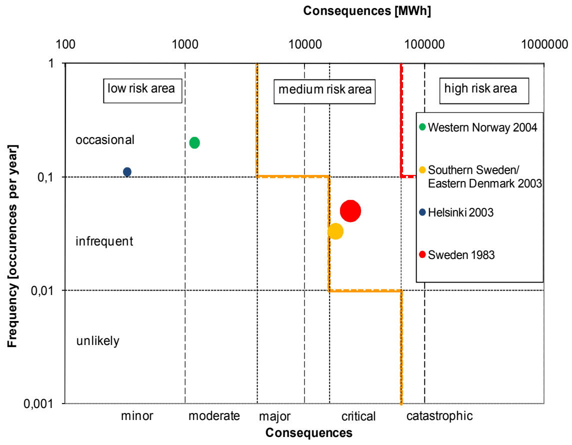

Fig.3 Risk diagram [6]

B. *Methods*

The bow-tie model is a concept for helping to structure and visualize the causes and consequences of unwanted (extraordinary) events as a basis for the risk and vulnerability analysis. For this analysis various methods are needed, covering the different aspects:

- Identification of threats and unwanted events
- Description of causes and probabilities (causal analysis)
- Classification of consequences (consequence analysis)
- Risk and vulnerability evaluation.

Previous studies indicate that there is no single methodology covering all these aspects, suitable for power system risk and vulnerability analysis of extraordinary events [9]. There is a need to combine different quantitative and qualitative methods. Examples of methods, supporting the different aspects, are shown in Fig. 4. The listed methods are regarded as the most relevant based on literature studies as well as experience from former and present work [3, 6, 8-10].

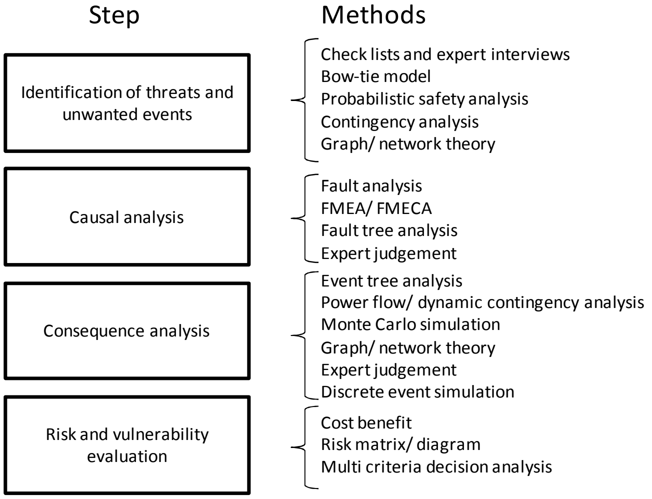

Fig. 4. Risk and vulnerability analysis – possible methods

Identification of threats and unwanted events includes identification of unwanted events and their corresponding hazards, threats and barriers. Experience so far indicates that this is one of the most challenging parts of risk and vulnerability analysis regarding identification of extraordinary (HILP) events. Several methods addressing the task are found in literature, some of them generic like graph/ network theory and some of them power system specific like probabilistic safety analysis adapted for power systems and contingency analysis. Our framework and the presented case study is (so far) based on experience, expert judgment and other “common sense” methods such as checklists, workshops, inspections, interviews, damage statistics and brainstorming for identification of threats and unwanted (extraordinary) events.

The purpose of the *causal analysis* is to find the causes leading to the identified unwanted events. For power system causal analysis relevant methods are fault tree analyses, reliability block diagrams and Markov analyses. “Common sense” methods are also used for causal analysis, especially expert judgment which is applied in our framework.

The purpose of the *consequence analysis* is to structure what happens (what is the performance of the critical infrastructure?) after an unwanted event has occurred. The consequence analysis might be carried out by generic methods such as event trees or discrete event simulation, or by specific methods for power system analysis. In the presented case study a combination of generic and power system specific methods is utilized, combining event trees and expert judgment with power flow and dynamic analyses. This makes sense since the process of operating the power system is an interaction between humans, the system and environment. Therefore no generic or specific method can provide answers alone.

Risk and vulnerability evaluation is the process in which judgments are made on the tolerability of risk and vulnerability. For power system risk and vulnerability evaluation generic methods like cost benefit and risk matrixes or diagrams (ref Fig. 3) can be used. Risk diagrams are applied in the framework and case study presented in this paper. As described in Section II vulnerability is closely related to the barriers. In this analysis step it is important to evaluate the existing barriers if these are sufficient and adequate and if new barriers are needed.

III. Case study

In this case study the risk and vulnerability of extraordinary events in a 420 kV transmission system is analyzed. The studied area is connected to neighboring areas via one AC connection and two DC connections, see Fig. 5.

Power system failures are considered, while energy and capacity balance are indirectly represented as a part of the power system operation, i.e. the operational state. The analyses are carried out by combining qualitative and quantitative techniques through the different steps described in Fig. 4.

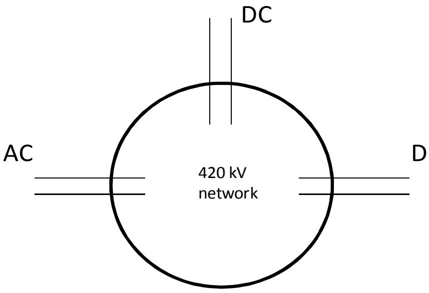

Fig. 5. Studied network – connection to other areas

The case study is carried out in close cooperation with the transmission system operator (TSO), and the analysis is described in the following sections.

1. Identification of threats and unwanted events

In this case study unwanted events, and corresponding threats that might lead to the unwanted events in certain operational states, are identified through a process including brainstorming and interviews with personnel at the TSOs control centre and planning department as well as power flow simulations. For the studied area three different *unwanted events* considered to be extraordinary were identified. The process of identifying the unwanted events has been both challenging and educational for the TSOs personnel. It has been difficult to find potentially severe events in the system, since both long-term and operational planning follow the (n-1) criterion and make sure that all *likely* events can be handled securely. In the following, one of the extraordinary events is described more in detail, illustrating the methodology.

According to expert judgment it is likely that the system will not withstand loss of the AC connection when import on the AC lines is higher than 900 MW. The unwanted event is therefore defined as "loss of both AC lines if import on AC lines is > 900 MW". See the corresponding bow-tie model in Fig. 6 using fault tree and event tree for the causal and consequence analyses respectively.

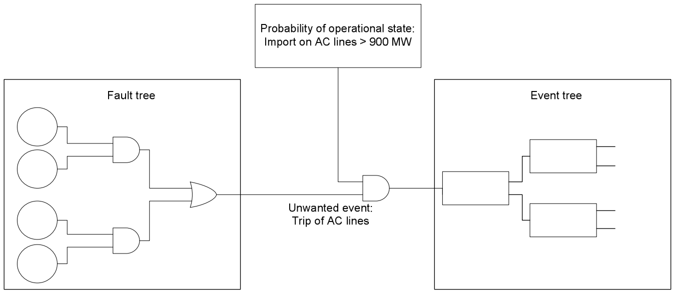
Probability of operational state:
Import on AC lines > 900 MW
Fault tree
Event tree
Unwanted event:
Trip of AC lines

Fig. 6. Bow-tie model for the selected unwanted event in the transmission system

The following *threats* or causes, leading to loss of both AC lines, are identified by expert judgment:

- Unwanted unselective breaker tripping
- Thunderstorm
- Sabotage
- Transportation accident
- Earth line breakage
- Galloping lines
- Station fault
- Power outage at feeding end.

These are not by themselves extraordinary events, but combined with a critical operational state (> 900 MW import on AC lines) and the fact that both lines are lost; the result might become an extraordinary event.

2. Causal analysis

The fault tree of "loss of both AC lines" is shown in Fig. 7. The basic events are based on the identified threats or causes and grouped as shown in the figure. All input data are based on combining fault statistics with expert judgment. Barriers on the "cause side" are not explicitly analyzed, but taken into account in the expert judgment. The resulting frequency of loss of both AC lines is calculated to 0.13 per year. The probability of the critical operating state is found from historical data and is 1.4%. Combining this information results in a frequency of "loss of both AC lines if import on AC lines is > 900 MW" of 0.00182 per year or a return period of 550 years.

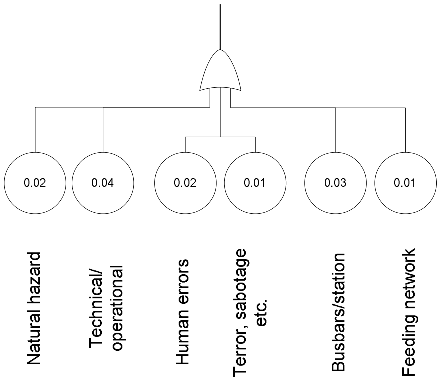

Fig. 7. Fault tree for the selected unwanted event in the transmission system

3. Consequence analysis

The consequence analysis for the unwanted event “loss of both AC lines if import on AC lines is > 900 MW” is carried out by using expert judgment in combination with power flow and dynamic analyses. If there were no barriers, the loss of 900 MW could not be handled by the system and a blackout would be inevitable. The resulting event tree is shown in Fig. 8 with the following barriers:

- HVDC emergency power
- Load shedding
- Controlled islanding.

Both HVDC emergency power and load shedding aim at reducing the unbalance between generation and load to avoid the frequency becoming too low, while controlled islanding is needed due to the loss of all AC connections.

The different consequences for this event are shown to the right in terms of load shedding and duration (from 15% when all barriers are successful to blackout (100%) when all barriers fail).

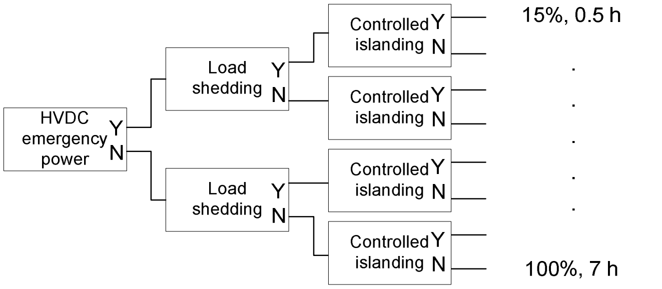

Fig. 8. Event tree for the selected unwanted event in the transmission system

The results from the consequence analysis are shown in the consequence diagram in Fig. 9 and risk diagram in Fig. 10 for all three unwanted events. “Event 3” corresponds to the one described above.

4. Risk and vulnerability evaluation

Two of the identified unwanted events have consequences considered by the TSO as “catastrophic”, while the third is “moderate”. Due to very low expected frequency the risk is categorized as medium or low for all three events. In the risk diagram the consequences in Fig. 8 are represented by a “blackout equivalent”, calculated as the equivalent number of hours with interruption of 100% of the load.

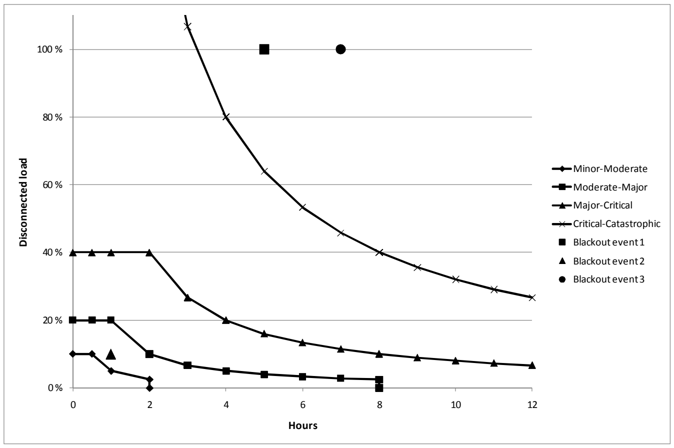

Fig. 9. Consequences of identified unwanted events

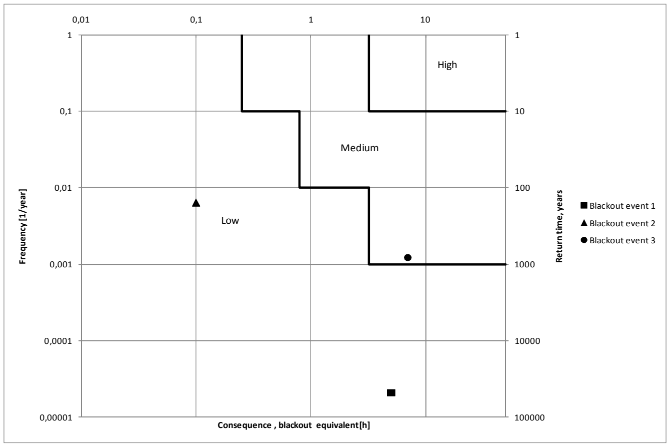

Fig. 10. Risk diagram of identified unwanted events

This case study clearly illustrates the “high societal impact and low probability to occur” nature of extraordinary events. Nevertheless, if the consequences are unacceptable, the extraordinary event must be taken into consideration, even if the risk is small.

5. Evaluation

The case study has shown that the presented framework is suitable for analysing extraordinary events. The process of identifying the extraordinary events is clearly important, and has in the case study shown to be challenging and educational to the TSO's personnel.

The flexibility within the framework in choosing analysis methods is useful in the highly complex task of thoroughly analysing the events.

The results from the risk analysis seem reasonable, and show that although having large consequences, the risk of the events range from medium to low. The details of the analyses can be used in reducing the future risk of both the studied and similar unwanted events.

However, it is hard to judge the overall risk of a power system using a small set of extraordinary events. The risk in the results reported here is small compared with an earlier study of the overall system risk that was based on expert judgement alone [6]. Possibly, there are two main reasons for this gap:

- In expert judgements of the overall risk, there might be a tendency of overestimating the risk
- The analysed set of identified extraordinary events is too small, either because there are many events with similar risks or some event with much higher risk than the ones analysed here.

IV. Conclusions and further work

The paper describes a framework for power system risk and vulnerability analysis largely based on expert judgment and supported by power flow and dynamic analyses, in order to capture also the less probable event with high impact. The bow-tie model is used to structure the analysis in terms of threats, unwanted events, barriers and consequences.

The framework is illustrated with a simplified real case study. The case study shows an example of a risk and vulnerability study of an extraordinary event where the consequence is unacceptable, but the risk is moderate due to the low probability for the extraordinary event to occur.

The case study and experience so far indicates that the identification of threats, causes and unwanted (extraordinary) events is one of the most challenging parts of a risk and vulnerability analysis. It is difficult to get the “full picture” by combining single events, and it is hard to think of the “unthinkable” even for experts.

Further work within the ongoing project will focus on methodology for dealing with extraordinary events in risk and vulnerability analyses. There is a need to develop and extend the traditional reliability analyses to take into account the effect of vulnerable operational states combined with extraordinary events in the grid. Indicators and models must be identified, events classified, and methods and tools must be further developed and tested. One of the main challenges is how to identify the vulnerable operational states and extraordinary events. There are several techniques described in literature that could be further investigated for this purpose, e.g. use of graph/ network theory or rare-event simulation [e.g. 11, 12].

V. References

[1] E. Johansson, K. Uhlen, A. Nybø, G. Kjølle, and O. Gjerde, "Extraordinary events - understanding sequence, causes and remedies," in *ESREL 2010*, 2010.

[2] R. Billinton and R. N. Allan, *Reliability Evaluation of Power Systems*. Norwell, MA: Kluwer, 1996.

[3] CIGRE Working Group C4.601, Review of the Current Status of Tools and Techniques for Risk-Based and Probabilistic Planning in Power Systems, CIGRE publication 434, ISBN: 978-2-85873-122-0

[4] G. T. Heydt, C. C. Liu, A. G. Phadke, and V. Vittal, "Solutions for the crisis in electric power supply," IEEE Computer Applications in Power, vol. 14, pp. 22-30, 2001.

[5] Y. V. Makarov and R. C. Hardiman, "Risk, reliability, cascading and restructuring," in IEEE Power Engineering Society General Meeting, 2003, pp. 1417-1429.

[6] G. L. Doorman, K. Uhlen, G. H. Kjolle, and E. S. Huse, "Vulnerability analysis of the Nordic power system," IEEE Transactions on Power Systems, vol. 21, pp. 402-410, Feb 2006.

[7] NordSecurEl, "Risk and vulnerability assessments for contingency planning and training in the Nordic electricity system. Final report," Statens Energimyndighet, EU EPCIP, Eskilstuna 2009.

[8] G. Kjølle, O. Gjerde, and A. Nybø, "A framework for handling high impact low probability (HILP) events," in CIRED Workshop 2010 Lyon, 2010.

[9] O. Gjerde, G. Doorman, G. H. Kjølle, A. Stefanini, M. Macera, P. Friessem, M. Stoewer, M. G. Jaatun, and O. H. Longva, "GRID Deliverable 7/GAP: Status overview and identified gaps WP2", 2007.

[10] G. Kjølle and O. Gjerde, "Integrated approach for security of electricity supply analysis", International Journal of Systems Assurance Engineering and Management, pp. 1-7, 2010.

[11] H. Jönsson, J. Johansson, H. Johansson, "Identifying Critical Components in Technical Infrastructure Networks", Journal of Risk and Reliability, Vol. 222, Part O, pp. 235-243, 2008.

[12] F. Fonteneau-Belmudes et.al, "Consequence driven decomposition of large-scale power system security analysis", *2010 IREP Symposium*.

VI. Biographies

Oddbjørn Gjerde received his MSc and PhD degrees in electrical engineering from the Norwegian University of Science and Technology (NTNU, former NTH), in 1993 and 1999 respectively. He has been with SINTEF Energy Research since 2000. He is presently a research scientist at SINTEF Energy Research, Department of Energy Systems. His special fields of interest are within security of electricity supply analysis, including reliability, risk and vulnerability assessment.

Gerd H. Kjølle (M’ 06) received her MSc and PhD degrees in electrical engineering from the Norwegian University of Science and Technology (NTNU, former NTH), in 1984 and 1996 respectively. She has been with SINTEF Energy Research since 1985. She is presently a senior research scientist at SINTEF Energy Research, Department of Energy Systems. She is also an adjunct professor at Norwegian University of Science and Technology, Dept. of Electric Power Engineering. Her special fields of interest include reliability and interruption cost assessment, energy systems planning and risk and vulnerability analyses.

Nina K. Detlefsen works in Systems Analysis at Energinet.dk. She studied operations research at the University of Aarhus, Denmark and the Norwegian University of Science and Technology. After working with research in decision support systems in agricultural sciences several years she joined the energy sector in 2006. Her special fields of interest include electric power systems, dispersed energy resources and modeling and optimizing energy system.

Geir Brønmo works in Systems Analysis at Energinet.dk. He studied operations research at the Norwegian University of Science and Technology. After working with revenue management in the airline industry for some years he joined the energy sector in 2008. His special fields of interest include market modelling and reliability analyses in electric power systems.