Evaluation of accident risks

Status and trends in risk analysis and evaluation

RÄDDNINGS
VERKET

Evaluation of accident risks

Status and trends in risk analysis and evaluation

Terje Aven

University of Stavanger
in cooperation with
Proactima AS

Contact at the Swedish Rescue Services Agency:
Omar Harrami, Research & Analysis Department, + 46 54 135359

Preface

Evaluation of risk involves many actors in society and is an important aspect of risk management. Often, it is assumed that the evaluations are optimal, rational, objective, fair and legitimate. Therefore, several theories and methods have been developed to improve and support risk evaluations for various contexts. Since these methods have evolved in different operational and research areas, where risk is comprehended in different ways, risk evaluation has become a heterogeneous field of knowledge. Also, methods that have been developed within different traditions of knowledge often end up in conflict with each other.

In order to create well-substantiated risk evaluations it is important to facilitate a discussion on different forms and perspectives of risk evaluation. The Swedish Rescue Services Agency is conducting work aimed at increasing knowledge and understanding of the evaluation of accident risks. By describing and discussing the foundations for risk evaluation it is possible to attain greater transparency and clarity of practice in different operational areas. As a first step in this work four reviews have been compiled, which describe the evaluation of accident risks in the following research areas: **economics**, **sociology**, **engineering/natural sciences** and **philosophy**. These reviews have been published in four reports:

- Economics: *Värdering av olycksrisker - Nationalekonomi*, order number P21-495/08 (in Swedish)
- Sociology: *Värdering av olycksrisker - Risksociologi och demokratisk riskvärdering*, order number P21-496/08 (in Swedish)
- Engineering/natural sciences: *Evaluation of accident risks - Status and trends in risk analysis and evaluation*, order number P21-497/08
- Philosophy: *Värdering av olycksrisker - Etik och riskvärdering*, order number P21-498/08 (in Swedish)

The results and issues raised in the review reports are discussed in a complementary report Värdering av olycksrisker - Fyra kunskapsområdens syn på riskvärdering (published 2009 by the Swedish Civil Contingencies Agency, MSB).

SWEDISH RESCUE SERVICES AGENCY
Research & Analysis Department

Contents

1. Introduction **4**

2. Risk perspectives **6**

3. Scientific basis **12**

4. Weaknesses and limitations of risk analysis **15**

Precision of a risk analysis. Uncertainty. Sensitivity analysis 15

Limitations of the Causal Chain Approach 16

5. Risk acceptance criteria and tolerability limits **19**

6. Further implications for risk assessment and risk management ... **22**

7. Conclusions **28**

References **29**

Bibliography **32**

1. Introduction

There is an enormous drive and enthusiasm in various industries, services and society as a whole nowadays to implement risk management. A recent review of the practical implementation of risk evaluation illustrates the range of applications across different sectors in Norwegian society and some of the challenges faced (Kierans 2007). There are high expectations, that risk management is the proper framework for obtaining high levels of performance. We see a lot of initiatives to establish adequate concepts and tools. However, the risk management discipline is young, and there are many difficult issues and challenges. These relate in particular to the foundation and use of risk analyses; how to express risk, how to handle uncertainties, how to analyse risk reflecting system specific information and how to specify and use risk acceptance criteria. These issues are addressed in this report. The purpose of the report is to review and discuss some key concepts and principles of risk analysis and risk evaluation, and point at key development trends and challenges.

Risk management is defined as all measures and activities carried out to manage risk (ISO 2005). Risk management deals with balancing the conflicts inherent in exploring opportunities on one hand, and avoiding losses, accidents, and disasters, on the other (Aven and Vinnem 2007). In order to support decision-making during design and operation, risk analyses are conducted. The analyses include identification of hazards and threats, cause analyses, consequence analyses and risk description. The results of the analyses are then evaluated. The totality of the analyses and the evaluations are referred to as risk assessments. Risk assessment is followed by risk treatment, which is a process involving the development and implementation of measures to modify risk, including measures designed to avoid, reduce ("optimize"), transfer or retain risk. Risk transfer means sharing with another party the benefit or loss associated with a risk. It is typically affected through insurance. The above terminology is in line with the ISO standard on risk management terminology (ISO 2005).

By carrying out a risk analysis we:

- Establish a risk picture
- Compare different alternatives and solutions in terms of risk
- Identify factors, conditions, activities, systems, components, etc. that are important (critical) with respect to risk
- Demonstrate the effect of various measures on risk.

This provides a basis for:

- Choosing between various alternative solutions and activities while in the planning phase of a system
- Choosing between alternative designs of a solution or a measure. What measures can be implemented to make the system less vulnerable in the sense that it can better tolerate loads and stresses?

- Drawing conclusions on whether various solutions and measures meet the stated requirements
- Setting requirements for various solutions and measures, for example, related to the performance of the preparedness systems
- Documenting an acceptable safety and risk level.

The strength of the risk analysis is that it systemizes available knowledge and uncertainties about phenomena, systems and activities that are being studies. What can go wrong, why, and what are the consequences? This knowledge and this uncertainty are described and discussed, and thereby we obtain a basis on which we can evaluate what is important and compare different solutions and measures.

The risk analysis and evaluation, however, also have some weaknesses/limitations and challenges. Some of these are discussed below. First we give some reflections on different risk perspectives and the scientific basis of risk analysis. We cannot discuss the weaknesses and limitations of risk analysis and risk evaluation without clarifying what risk is and how we should express risk.

The discussion is to a large extent based on Aven (2008b), as well as Aven (2008a) and Aven and Renn (2008a,b).

2. Risk perspectives

There is no agreed definition of risk. Risk is understood as an expected value, a probability distribution, as uncertainty and as an event. Some definitions are (Aven 2008a, Aven and Renn 2008a):

1. Risk equals the expected loss (Willis 2007)
2. Risk equals the expected disutility (Campbell 2005)
3. Risk is the probability of an adverse outcome (Graham and Weiner 1995)
4. Risk is a measure of the probability and severity of adverse effects (Lowrance 1976)
5. Risk is the combination of probability of an event and its consequences (ISO 2002)
6. Risk is defined as a set of scenarios s_i, each of which has a probability p_i and a consequence c_i (Kaplan and Garrick 1981, Kaplan 1991)
7. Risk is equal to the combination of possible events/consequences and associated uncertainties (Aven 2007a)
8. Risk refers to uncertainty of outcome, of actions and events (Cabinet Office 2002)
9. Risk is a situation or event where something of human value (including humans themselves) has been put at stake and where the outcome is uncertain (Rosa 1998)
10. Risk is an uncertain consequence of an event or an activity with respect to something that human value (Renn 2005).
11. Uncertainty about and severity of the consequences of an activity, with respect to something that humans value (Aven and Renn 2008a).
12. Risk refers to situations with known probabilities for the randomness the decision-maker is faced with (Knight 1921, Douglas 1983)

It is common to refer to risk as probability multiplied by consequences (losses), i.e. what is called the expected value in probability calculus. If C is a quantity of interest, for example the number of future attacks, the number of fatalities, the costs etc., an expected value would be a good representation of risk if this value is approximately equal to C, i.e. $EC \approx C$. But since C is unknown at the time of the assessment, how can we be sure that this approximation would be accurate? Can the law of large numbers be applied, expressing that the empirical mean of independent identically distributed random variables converges to the expected value when the number of variable increases to infinity? Or the portfolio theory (Levy and Sarnat 1994) saying that value of a portfolio of projects is approximately equal to the expected value, plus the systematic risk (uncertainties) caused by events affecting the whole market?

Yes, it is likely that if C is the sum of a number of projects, or some average number, our expected value could be a good prediction of C. Take for example the number of fatalities in traffic in a specific country. From previous years we have data that can be used to accurately predict the number of fatalities next year (C). In Norway about 250 people were killed last year, and using this number as EC and predictor for the coming year, we would be quite sure that this number is close to the actual C.

However, in many cases the uncertainties are much larger. Looking at the number of fatalities in Norway caused by terrorist attacks the next year, the historical data would give a poor basis. We may assign an EC but obviously EC could be far away from C. The accuracy increases when we extend the population of interest. If we look at one unit (e.g. country) in isolation the C numbers are in general more uncertain than if we consider many units (e.g. countries). Yet, there will always be uncertainties, and in a world where the speed of change is increasing, relevant historical data are scarce and will not be sufficient to obtain accurate predictions.

Nonetheless, some researchers define risk by the expected values. Consider the terrorism case discussed in (Willis 2007). Willis defines risk as follows:

> Terrorism risk: The expected consequences of an existent threat, which for a given target, attack mode, target vulnerability, and damage type, can be expressed as
>
> Risk = P(attack occurs) · P(attacks results in damage | attacks occurs) · E[damage | attacks occurs and results in damage]

Willis refers to Haimes (2004) who highlights that expected value decision-making is misleading for rare and extreme events. The expected value (the mean or the central tendency) does not adequately capture events with low probabilities and high consequences. Nonetheless, Willis represents risk by the expected value as the basis for his analysis. The motivation seems to be that the expected value provides a suitable practical approach for comparing and aggregating terrorism risk, as it is based on just one number.

For terrorism risk, where the possible consequences could be extreme and the uncertainties in underlying phenomena and processes are so large, it is obvious that the expected value may hide important aspects of concern for risk management. The expected value can be small, say 0.01 fatalities, but extreme events with millions of fatalities may occur, and this needs special attention.

One way of representing this aspect of risk is to specify the probability of an event resulting in large damages, P(large damages), for example the probability of an event occurring leading to a large number of fatalities. Willis notes that estimates of such probabilities of the worst-case outcomes, captured in the tail of the distribution of consequences, will be very dependent upon assumptions when considering events like terrorism where there are large uncertainties about events and limited historical information.

However, also estimates of the risk defined by the expected value will be strongly dependent on the assumptions made. Willis acknowledges this and in several places in his paper remarks that there are large uncertainties in the risk estimates. Willis' thinking seems to be based on an idea that there exist a true probability and a true risk. He speaks about errors in risk estimates, which means that there must be a reference point (a true value) to judge deviation. For the probability of attack Willis emphasizes that this probability is uncertain and that one should keep in mind that it can also be represented by a probability distribution, not a point estimate.

Certainly, if the risk perspective adopted is based on the idea of a true risk, the uncertainties in the estimates would be extremely large in a terrorism risk case. And these uncertainties need to be taken into account in the risk management. Willis claims that the conclusions drawn in his study are robust to these uncertainties, but this is hard to see, and it is obvious that in general the uncertainties would be so large that the risk management would be affected.

The idea of a true probability fits into a classical relative frequency paradigm; a probability is interpreted as the relative fraction of times the events occur if the situation analyzed were hypothetically "repeated" an infinite number of times. The underlying probability is unknown, and is estimated in the risk analysis. But is such an interpretation meaningful for the terrorism risk case? Can P(attack occurs) be understood by reference to such a thought-constructed repeated experiment? No, it can not. It has no meaning.

The alternative, and our recommended perspective in this report (the so-called Bayesian perspective), is to consider probability as a measure of uncertainty about events and outcomes (consequences), seen through the eyes of the assessor and based on some background information and knowledge. However, probability is not a perfect tool for this purpose. The assigned probabilities are conditional on specific background knowledge, and they could produce poor predictions.

This leads to our conclusion that the main component of risk is uncertainty and not probability; uncertainty about attacks occurring and about the resulting damages. Surprises relative to the assigned probabilities may occur, and by just addressing probabilities such surprises may be overlooked (Aven 2007a, 2008a,b, Taleb 2007).

However, risk should not be defined as uncertainty as in (8) above. Consider the number of fatalities in traffic next year in a specific country. Then the uncertainty is rather small, as the number of fatalities shows rather small variations from year to year. Hence as risk is defined by uncertainty we must conclude that the risk is small, even though the number of fatalities is many thousands each year. Clearly, this definition of risk fails to capture an essential aspect, the severity or importance of the possible consequences.

Take an extreme case where only two outcomes are possible, 0 and 1, corresponding to 0 and 1 fatality, and the decision alternatives are A and B, having uncertainty (probability) distributions (0.5,0.5), and (0.0001, 0.9999), respectively. Hence for alternative A there is a higher degree of uncertainty than for alternative B, meaning that risk according to this definition is higher for alternative A than for B. However, considering both dimensions, both uncertainty and the consequences, we would of course judge alternative B to have the highest risk as the negative outcome 1 is almost certain to occur.

This leads to our recommended risk perspective (ref. definition 7 above).

> By risk we understand the combination of i) possible events A and the consequences of these events C, and ii) the associated uncertainties U (about what will be the outcome), i.e. (C, U). For simplicity, we write only C, instead of A and C. (I)

We may rephrase this definition by saying that risk associated with an activity is to be understood as (Aven and Renn 2008a) (ref. definition 11 above):

> Uncertainty about and severity of the consequences of an activity, where severity refers to intensity, size, extension, and so on, and is with respect to something that humans value (lives, the environment, money, etc). Losses and gains, for example expressed by money or the number of fatalities, are ways of defining the severity of the consequences. (I')

Hence risk equals uncertainty about the consequences of an activity seen in relation to the severity of the consequences. Note that the uncertainties relate to the consequences C; the severity is just a way of characterising the consequences.

The main features of this definition are illustrated in Figure 1.

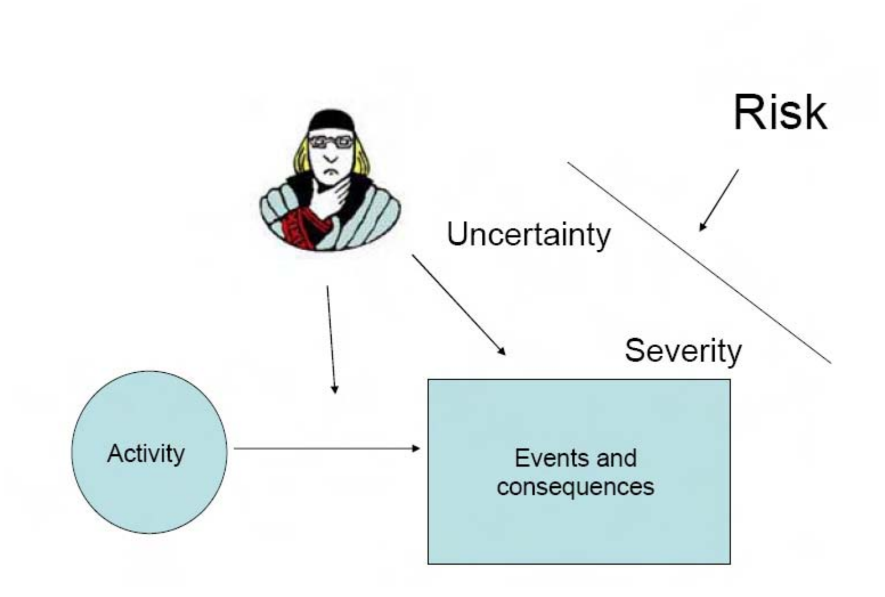


Figure 1: Illustration of the risk definitions (I) and (I')

A description of risk will thus contain the components (C, U, P, K), where C refers to the consequences, U uncertainties, P probability and K the background knowledge. Often we add C*, which is a prediction of C. By a prediction we mean a forecast of which value this quantity will take in real life. We may use one number, but often we specify a prediction interval [a, b] such that C will be in the interval with a certain probability (typical 90% or 95%). Often such intervals are derived conditional that the event A has occurred.

If we say that the probability of an event A given the background knowledge K is 10%, i.e. P(A | K) = 0.10, this means that we judge it just as likely that the event A will occur as it is to draw a particular ball from a urn containing 10 balls. The uncertainty in whether the event A will occur or not, is comparable to the uncertainty in whether or not the particular ball in the urn will be drawn.

The definition of vulnerability follows the same logic as that of risk. By vulnerability we understood the combination of possible consequences and the associated uncertainty, given the occurrence of the initiating event A, i.e. (C, U |A), using the notation introduced above. A description of vulnerability thus covers the following elements: (C, C*, U, P, K | A).

This risk perspective means a broad approach to risk as discussed in more detail in Section 4. To evaluate the seriousness of risk and conclude on risk treatment, we need to see beyond the expected values and the probabilities. This is also in line with other approaches, including the UK Cabinet office approach (Cabinet Office 2002) and the risk governance framework (Renn 2005).

We refer to Aven and Renn (2008a) for a discussion of the differences between the definition (11) and Rosa (1998)'s definition (9) and Renn's (2005) definition (10). A main point is that the restriction of the risk concept to events and consequences without consideration of uncertainties, means that fundamental concepts such as risk evaluation and risk perception need to be reinterpreted, and a non-intuitive language is introduced. For example, we cannot talk about high risks and acceptable risk.

Our definition does not include utilities as in definition 2). The preferences of the decision maker are not a part of the risk concept. There will be a strong degree of arbitrariness in the choice of the utility function, and some decision makers would also be reluctant to specify the utility function as it reduces their flexibility to weigh different concerns in specific cases.

In economic applications a distinction has traditionally been made between risk and uncertainty, based on the availability of information. Under risk the probability distribution of the performance measures can be assigned objectively (def. 12), whereas under uncertainty these probabilities must be assigned or estimated on a subjective basis (Douglas (1983). This definition goes back to Knight (1921). Although this definition is often referred to, it is not so often used in practice. The problem is of course that we seldom have known distributions, and then we cannot refer to the risk concept. The Knightian definition violates the intuitive interpretation of risk, which is related to situations of uncertainty and lack of accurate predictions.

An alternative approach for analysing intelligent attacks is to use game theory, see Guikema (2007) and the references therein. Using this approach possible interactions are taken into account, but strong assumptions need to be made related to the attackers' behaviour and decision-making. We refer to Guikema and Aven (2007).

3. Scientific basis

We consider a risk problem where the uncertainties are large. To be specific think above terrorism example. If the goal of the risk analysis is to obtain accurate estimates of some true risk, we can quickly conclude that risk analysis fails as a scientific method. Referring to the previous section, we can conclude that the classical approach to risk analysis does not work in situations involving large uncertainties. The uncertainties of the risk estimates are too large.

Alternatively, we may consider risk analysis as a tool for assessing uncertainties about risk and risk estimates. Risk analysis is then not about bounding and reducing uncertainties, but to describe uncertainties. Two prevailing approaches for describing the uncertainties are:

1. Traditional statistical methods such as confidence intervals
2. The probability of frequency approach, i.e. assessing epistemic uncertainties about the risk by means of subjective probabilities. In this approach there are two levels of probability introduced; i) the relative frequency interpreted probabilities reflecting variation within populations and ii) the subjective probabilities reflecting the analyst's uncertainty what the correct relative frequency probabilities are (see e.g. Kaplan and Garrick (1981) and Aven (2003)). In Garrick et.al. (2004) the probability of frequency approach is suggested for risk analysis of terrorist attacks. Garrick et al. (2004) refers to a probability distribution saying for example that there is a probability of 20% that the attackers would succeed in 10% of their attacks.

However, confidence intervals would not work in this setting as we do not have sufficient amount of relevant data. Even if some data are available, the traditional statistical approach is problematic. To apply the approach, probability models like the normal distribution and the log normal distribution need to be specified, but in practice it is difficult to determine the appropriate distribution. Our historical data may include no extreme observations, but this does not preclude such observations to occur in the future. Statistical analysis, including Bayesian statistics, is based on the idea of similar situations and if "similar" is limited to the historical data, the population considered could be far too small or narrow. However, by extending the population, the statistical framework breaks down. There is no justification for such an extended probability model. The statistician needs a probability model to be able to perform a statistical analysis, and then he will base his analysis on the data available. Taleb (2007) refers to the worlds of mediocristan and extremistan to explain the difference between the standard probability model context and the more extended population required to reflect surprises occurring in the future, respectively. Without explicitly formulating the thesis, Taleb (2007) is saying that we have to see beyond the historically based probability models.

The ambition of the probability of frequency approach is to express the epistemic uncertainties of the probability p of an attack, and take into account all relevant factors causing uncertainties. The analysis may produce a 90% credibility interval for p, [a, b], saying that the analyst is 90% confident that p lies in the interval [a, b]. In practice it is difficult to perform a complete uncertainty analysis following this approach. In theory an uncertainty distribution on the total model and parameter space should be established, which is impossible to do. So in applications only a few marginal distributions on some selected parameters are normally specified, and therefore the uncertainty distributions on the output probabilities are just reflecting some aspects of the uncertainty. This makes it difficult to interpret the produced uncertainties.

The validity of the risk analysis when adopting the probability of frequency approach can also be questioned, from a different angle. As questioned in the previous section, is the relative frequency interpreted probability of an attack p really the quantity of interest? Our goal is to express the risk of an activity or system, but in this approach we are concerned about the average performance of a thought-constructed population of similar situations. Are these quantities meaningful representations of the activity or system being studied? Clearly, when for example looking at the total activity of a society or a nation, it is hard to understand the meaning of such a constructed infinite population. If we are to assess uncertainties concerning average performance of quantities of such populations, it is essential that we understand what they mean.

According to our recommended approach, probability is a measure of uncertainty seen through the eyes of the assessor, and based on a background knowledge. The aim of risk analysis in this context is to assess and express uncertainties about unknown quantities, using probabilities. In traditional text-book Bayesian analysis the quantities focused are fictional parameters as in the probability of frequency approach discussed above. In the following we restrict attention to Bayesian approaches where focus is on predictions and uncertainty assessments of observable quantities (Aven 2003, 2007a). Examples of observable quantities are costs, number of fatalities, and the occurrence of an event, for example an attack.

In the probability of frequency case we are uncertain about parameters, whereas for these Bayesian approaches, we are uncertain about observables. Hence the validity problem raised for the probability of frequency approach is not relevant for these Bayesian approaches. The observables are directly expressing the interesting features of the actual system, for example the number of fatalities, the costs etc. Of course, the observables addressed should be informative in the sense that the results of the analysis support the decision-making. If this is not the case, there is obviously a validity problem.

For further reading on this topic, see Aven and Knudsen (2008).

We see that the scientific basis of risk assessments can be questioned, depending on the risk perspective adopted. The implications for risk management we discuss in the next section.

4. Weaknesses and limitations of risk analysis

Precision of a risk analysis. Uncertainty. Sensitivity analysis

If one has a large and relevant database, the probabilities derived from it could be precise in the sense that they may be able to provide accurate predictions of future events. For example, assume that one has observed 200 failures in a population of 10 000 units of type T over a one year period. The derived probability of failure for an arbitrarily chosen unit is then 2%, and we will predict for example 20 failures per thousand units. We can express the uncertainty, for example, using a 95% prediction interval: [11, 29]. The number of failures will lie within this interval with a 95% probability. To establish this interval, let X denote the number of failures among 1000 units. Then X has a binomial distribution, which can be approximated by a normal distribution with mean 20 and standard deviation 4.4, and this gives $P(11 \leq X \leq 29) = 0.95$. See a text-book in statistics.

In a risk analysis context, we often focus on rare events, for example, the occurrence of a fatal accident, an accident that causes impairment of a main safety function, etc. We have only one unit or activity, and we are able to give a good prediction about the future: no fatal accidents will occur the next year. Fortunately, such a prediction will normally provide correct results. The risk analysis, however, should also express the likelihood associated with whether the event will occur. This raises the question about precision in the probability assignment, as discussed in Section 3.

Following our recommended risk perspective, probability is used to express the analysts' uncertainty concerning whether the event will occur or not. If it is 10%, then the uncertainty is the same as drawing a particular ball from an urn containing 10 balls. It makes no sense discussing uncertainty in this number, but the assigned number depends, of course, on the assumptions and suppositions on which the analysis is built, and on who is carrying out the analysis. A critical question regarding the precision of the risk analysis results is thus in order.

The conclusion is that sensitivity analyses must be carried out in order to show how the results depend on various conditions and assumptions. Note that sensitivity analysis is not an analysis of uncertainty, as many seem to think. Sensitivity analysis highlights the importance of key quantities (parameters), and can provide a basis for assessing uncertainty. However, as such they do not provide any conclusions on uncertainties.

Many risk analyses today are characterized either by silence on the subject, or by general statements such as:

> The analyses are based on the “best estimates” obtained by using the company's standards for models and data. It is acknowledged that there are uncertainties associated with all elements in the analysis, from the hazard identification to the models and probability calculations. It is concluded that the precision of the analysis is limited, and that one must take this into considerations when comparing the results with the risk acceptance criteria and tolerability limits.

The above statement is not very convincing, and it is not relevant for the recommended risk perspective in this report. It is obvious that there is no clarity regarding what the analyses express, and what uncertainty means in a risk analysis context.

In any event, does this acknowledgment - that a considerable amount of uncertainty exists - affect the analyses and the conclusions? Only very rarely! Our impression is that one writes such statements just to meet a requirement, and then they are put aside. This says a lot about the quality of the analyses.

In cases where we have observed data, we can compare the risk figures with these. Do the risk figures give reasonable predictions of the number of events? If the analysis yields a probability figure that, for example, indicates 10 leakages of a certain category over 20 years, but observed data for similar systems is an order of magnitude lower, then this must be discussed. Is the result reasonable, or is there a need to have a closer look at the uncertainty assessments? Rarely, or practically never, do we see that such reflections are carried out in risk analyses today.

The lack of precision in the analysis is important for how the risk analysis can, and should, be used. There is, for example, no use in applying the analysis for precise comparisons of the results with given limits to decide whether the risk is acceptable or not. If we wish to compare with a criterion of $1 \cdot 10^{-4}$, we cannot in practice distinguish between the results from risk analyses that yield values of, for example, $2 \cdot 10^{-4}$, and $0.5 \cdot 10^{-4}$. The results are in the same order of magnitude as the criterion, and there is no need to say more.

Limitations of the Causal Chain Approach

The traditional risk analysis approach can be viewed as a special case of system engineering (Haimes 2004). This approach, which to a large extent is based on causal chains and event modelling, has been subject to strong criticism. Many researchers argue that some of the key methods used in risk analysis are not able to capture “Systemic accidents”. Hollnagel (2004), for example, argues that to model systemic accidents it is necessary to go beyond the causal chains - we must describe system performance as a whole, where the steps and stages on the way to an accident are seen as parts of a whole rather than as distinct events. It is not only interesting to model the events that lead to the occurrence of an accident, which is done in for example event and fault trees, but also to capture the array of factors at different system levels that contribute to the occurrence of these events. Leveson (2007) makes her points very clear:

> Traditional methods and tools for risk analysis and management have not been terribly successful in the new types of high-tech systems with distributed human and automated decision-making we are attempting to build today. The traditional approaches, mostly based on viewing causality in terms of chains of events with relatively simple cause-effect links, are based on assumptions that do not fit these new types of systems: These approaches to safety engineering were created in the world of primarily mechanical systems and then adapted for electro-mechanical systems, none of which begin to approach the level of complexity, non-linear dynamic interactions, and technological innovation in today's socio-technical systems. At the same time, today's complex engineered systems have become increasingly essential to our lives. In addition to traditional infrastructures (such as water, electrical, and ground transportation systems), there are increasingly complex communication systems, information systems, air transportation systems, new product/process development systems, production systems, distribution systems, and others.
>
> The limitations of the traditional models and approaches to managing and assessing risk in these systems make it difficult to include all factors contributing to risk, including human performance and organizational, management and social factors; to incorporate human error and complex decision-making; and to capture the non-linear dynamics of interactions among components, including the adaptation of social and technical structures over time.

Leveson argues for a paradigm-changing approach to safety engineering and risk management. She refers to a new alternative accident model, called STAMP (System- Theoretic Accident Modelling and Processes).

A critical review of the principles and methods being used is of course important, and the research by Hollnagel, Leveson, Rasmussen (1997) and others in this field adds valuable input to the further development of risk analysis as a discipline. Obviously we need a set of different approaches and methods for analysing risk. No approach is able to meet the expectations with respect to all aspects. The causal chains and event modelling approach has shown to work for a number of industries and settings, and the overall judgment of the approach is not as negative as Leveson expresses.

Furthermore, the causal chains and event modelling approach is continuously improved, incorporating human, operational and organizational factors, see e.g. I-Risk (Papazoglou et al. 2003), ARAMIS (Dujim and Goossens, 2006), the BORA project (Aven et al. 2006), the SAM approach Paté-Cornell and Murphy 1996), the HCL method (Røed et.al. 2008, Mohaghegh et al. 2008), as well as Léger et.al. (2008), Ale et.al. (2008) and Luxhøj et.al. (2001). It is not difficult to point at limitations of these approaches, but it is important to acknowledge that the suitability of a model always has to be judged by reference to its ability to represent the real world, but also its ability to simplify the world. All models are wrong, but they can still be useful, to use a well-known phrase.

The approach taken in Aven (2008a, b) and reflected in this report is partly based on the causal chains and event modelling. However, we acknowledge the limitations of this approach, as well as other aspects of the analyses, and add alternative qualitative tools to see beyond these limitations. Insights provided by this alternative research paradigm can be used to strengthen the risk picture obtained by the more traditional approach. The framework adopted in Aven (2008a, b) allows for such an extended knowledge basis. In fact, it encourages the analysts to search for such a basis.

5. Risk acceptance criteria and tolerability limits

To manage risk, and in particular safety, it is common to use a hierarchy of goals, criteria and requirements, such as:

A. Overall ideal goals, for example "our goal is to have no accidents".
B. Risk acceptance criteria (defined as upper limits of acceptable risk) or tolerability limits, controlling the accident risk, for example "the individual probability of being killed in an accident shall not exceed 0.1%".
C. Requirements related to the performance of safety systems and barriers, such as a reliability requirement for a safety system.
D. Requirements related to the specific design and operation of a component or subsystem, for example the gas detection system.

According to the standard procedures for using such goals, criteria and requirements, they are to be specified before alternatives are generated and subsequently analysed. The point is to look for what to obtain before looking for possible ways of implementation. For example, the Norwegian offshore petroleum regulations state that risk acceptance criteria (expressed as upper limits of acceptable risk) should be developed, before the risk analyses are carried out (PSA 2001, Aven and Vinnem 2007). Note that we in the following, when using the term "risk acceptance criteria", always have in mind such upper limits.

Are such criteria appropriate for managing risk? Consider the following criterion: "The probability of having an oil spill during one year of operation causing an environmental damage having a restitution period of more than z years, should not exceed $1 \cdot 10^{-x}$".

At the political level it is obvious that it would not be possible to establish consensus about such a limit. Different parties would have different preferences. But for the Government it should be possible to establish such a number? Say that it would make an attempt to do this. And suppose that it considers two options, a weak limit, say, $1 \cdot 10^{-3}$, and a strong limit, say, $1 \cdot 10^{-4}$. What limit should it choose? The answer would be the weak limit, as the strong limit could mean lack of flexibility in choosing the overall best solution. If the benefits are sufficiently large, the level $1 \cdot 10^{-3}$ could be acceptable. Following this line of argument, the use of such limits leads to the formulation of weak limits, which are met in most situations. Risk analysis is then used to verify that the risk is acceptable in relation to these weak limits. It is to a large extent a waste of money; the conclusion is obvious.

At the operational level, the same type of arguments will apply. The oil company is to determine an acceptance criterion, and it faces the same type of dilemmas as above. Why should it specify strong limits? It would restrict the company from obtaining the overall best solution. The result is that weak limits are specified and risk analyses play the role of verification, a role that does not add much value.

If a high level of safety is to be obtained, other mechanisms than risk acceptance criteria need to be implemented. If such criteria are established, they give a focus on obtaining a minimum safety standard - no drive for improvement and risk reduction.

The ALARP principle (ALARP: As Low as Reasonably Practicable) represents such a mechanism. The ALARP principle expresses that the risk should be reduced to a level that is as low as reasonably practicable. A risk reducing measure should be implemented provided it cannot be demonstrated that the costs are grossly disproportionate relative to the gains obtained (HSE 2001). Risk assessments play an important in ALARP processes, as many risk reduction decisions need to be supported by risk assessments. Risk must be described and the effect of risk reducing measures determined.

We conclude that care has to be shown when introducing risk acceptance criteria. Risk should not be considered in isolation. We do not accept the risk, but options that entail some level of risk among their consequences (Fischhoff et al 1981, p.3). Principally speaking, a requirement (criterion) related to risk and safety cannot be isolated from what the solution and measure mean in relation to other attributes, in particular costs. It is impossible to know what should be the proper requirement without knowing what it implies and what it means when it comes to cost, effect on safety etc. In other words, first we need the alternatives. Then we can analyse and evaluate these, and finally we should make a decision.

This is our theoretical position. It applies to all levels of limits (within category B and C above) from the high level performance of an industry, a plant and so on, to the detailed equipment level. In practice however, there is a need for a more pragmatic thinking about the use of such criteria and requirements, in particular for the more detailed requirements, as explained in the following.

When designing a complex system like an offshore installation we need to introduce some simplifications. We simplify the description of the installation by saying that it consists of several systems (system is here used in a broad sense, covering aspects of structure, layout, emergency preparedness, etc). For all these systems there are possible detailed arrangements and measures. However, in an early design phase it is not feasible to specify all these arrangements and measures in detail, and instead we use some sort of performance characterisation. Typically, these will be industry standards, established practice and descriptions of the performance of the system, given by reliability, effectiveness (capacity) and robustness. In other words, instead of specifying in an accurate way, what system we need, we specify the performance of the system. Thus we have basically three levels of specification:

1. The installation comprising its arrangements and measures (this is the way the installation will be in operation)
2. The installation described by systems defined through a form of performance characterisations
3. Systems described by specific arrangements and measures.

Level 1 is the ultimate level, the installation as it would be in the future. In an early planning phase, we may use Level 2, and specify systems and their performance. In detailed design, we move to Level 3 and specify the detailed and specific arrangements and measures for the relevant system. Specifying performance requirements related to Level 3 is not a problem, since they simply express properties of the arrangements and measures. The interesting question is whether we can justify the use of performance requirements at Level 2. Our conclusion is that such requirements are necessary for the practical execution of the project. We need some starting point for the specification of the performance for the system level. Consider the following example:

> Safety system reliability requirement: “Safety system S shall have a maximum failure on demand probability equal to 1%”

Instead of a sharp level, ranges may also be used, such as the categorisation used for Safety Integrity Level (SIL) requirements, in accordance with IEC 61511, for example a failure probability in the range 10% - 1%. The engineering process will produce a specific system layout that should meet this requirement. The starting point for choosing a certain requirement could be historical data, standards, or the desire to achieve a certain risk level or improvement.

However, for the 1% requirement to be meaningful it must not be seen as a sharp line; we should always look for alternatives and then evaluate their performance. Whether the analysis team calculates a reliability of 0.2%, 0.5% or 2% is not so important - depending on the situation we may accept all these levels. The interesting question is how the alternatives perform relatively, concerning reliability, costs and other factors. The number 1% must be seen as a starting point for further optimisation.

To summarise: One should avoid using pre-defined risk acceptance criteria for managing risk at a high system level, such as an industry or a plant. On a more detailed system level, criteria and requirements need to be introduced to simplify the project development process. However, the criteria and requirements defined should not be seen as strict limits. There should always be a drive for generating overall better alternatives.

6. Further implications for risk assessment and risk management

Apostolakis and Lemon (2005) adopt a pragmatic approach to risk analysis and risk management, acknowledging the difficulties of determining probabilities for an attack. Ideally, they would like to implement a risk-informed procedure, based on expected values. However, since such an approach would require the use of probabilities that have not been "derived rigorously", they see themselves forced to resort to a more pragmatic approach.
This is one possible approach when facing problems of large uncertainties. The risk analyses simply do not provide a sufficient solid basis for the decision-making process. Others conclude differently, however, as already mentioned Garrick et al. (2004) recommend the use of the probability of frequency approach, despite the problems of implementing this approach as discussed in the previous section (see also Aven (2007a)). A full probabilistic analysis as in the probability of frequency approach, cannot in our view be justified. In a risk evaluation we need to see beyond the computed risk picture in the form of the summarising probabilities and expected values, as discussed above. Traditional quantitative risk analyses fail in this respect. We acknowledge the need for analysing risk, but question the value added by performing traditional quantitative risk analyses in cases of large uncertainties. The arbitrariness in the numbers produced could be significant, due to the uncertainties in the estimates or as a result of the uncertainty assessments being strongly dependent on the analysts.

We should acknowledge that risk cannot be accurately expressed using probabilities and expected values. A quantitative risk analysis is in many cases better replaced by a more qualitative approach, as discussed above (Aven 2008a,b). We may refer to it as a semi-quantitative approach. The basic features of the approach can be summarised as follows:

- A broad qualitative risk picture is established highlighting
    - Potential hazards/threats and accident scenarios
    - Barriers and the effectiveness of these barriers
    - Risk influencing factors and possible risk reducing measures
    - Uncertainties in phenomena and processes
    - Vulnerabilities
    - Special features of the consequences
    - Manageability factors. To what extent is it possible to control and reduce the uncertainties and thereby arrive at the desired outcome? Some risks are more manageable than others in the sense that there is a greater potential to reduce risk. An alternative can have a relatively large calculated risk under certain circumstances, but the manageability could be good and could result in a far better outcome than expected.

- Crude risk categorisations are defined based on this risk picture, reflecting
    - Probabilities/frequencies of hazards/threats
    - Expected losses given the occurrence of such a hazard/threat
    - Factors that could create large deviations between expected outcomes and the actual outcomes (uncertainties, vulnerabilities)
- Evaluations of the risk picture and categorisations to compare alternatives and make judgments about risk acceptance.

Quantifying risk using risk indices such as the expected number of fatalities gives an impression that risk can be expressed in a very precise way. However, in most cases, the arbitrariness is large, and our semi-quantitative approach acknowledges this by providing crude risk numbers, including analyses of the factors that can cause “surprises” relative to the probabilities and the expected values. We are not negative to detailed risk quantification as such, but quantification often requires strong simplifications and assumptions and, as a result, important factors could be ignored or given too little (or much) weight. In a qualitative or semi-quantitative analysis a more comprehensive risk picture can be established, taking into account underlying factors influencing risk. In contrast to the prevailing use of quantitative risk analyses, the precision level of the risk description is in line with the accuracy of the risk analysis tools. In addition, risk quantification is very resource demanding. We need to ask whether the resources are used in the best way. We conclude that in many cases more is gained by opening up for a broader, more qualitative approach, which allows for considerations beyond the probabilities and expected values.

For problems with large uncertainties, risk assessments could support decision making, but other principles, measures and instruments are required. We first point at the cautionary principle, which is a basic principle in risk and safety management, expressing that in the face of uncertainty, *caution* should be a ruling principle, for example by not starting an activity, or by implementing measures to reduce risks and uncertainties (HSE 2001, Aven and Vinnem 2007). The level of caution adopted will of course have to be balanced against other concerns such as costs. However, all industries would introduce some minimum requirements to protect people and the environment, and these requirements can be considered justified by the reference to the cautionary principle. The precautionary principle may be considered a special case of the cautionary principle, as it is applicable in cases of *scientific uncertainties* (Sandin 1999, Löfstedt 2003, Aven 2006).

It is prudent to distinguish management strategies for handling the risk agent (such as a chemical or a technology) from those needed for the risk absorbing system (such as a building, an organism or an ecosystem) (Renn 2005, Aven and Renn 2008b). With respect to risk absorbing systems robustness and resilience are two main categories of strategies/principles. *Robustness* refers to the insensitivity of performance to deviations from normal conditions. Measures to improve robustness include inserting conservatisms or safety factors as an assurance against individual variation, introducing redundant and diverse safety devices to improve structures against multiple stress situations, reducing the susceptibility of the target organism (example: iodine tablets for radiation protection), establishing building codes and zoning laws to protect against natural hazards as well as improving the organisational capability to initiate, enforce, monitor and revise management actions (high reliability, learning organisations).

With respect to risk absorbing systems, an important objective is to make these systems resilient so they can withstand or even tolerate surprises. In contrast to robustness, where potential threats are known in advance and the absorbing system needs to be prepared to face these threats, *resilience* is a protective strategy against unknown or highly uncertain hazards. Instruments for resilience include the strengthening of the immune system, diversification of the means for approaching identical or similar ends, reduction of the overall catastrophic potential or vulnerability even in the absence of a concrete threat, design of systems with flexible response options and the improvement of conditions for emergency management and system adaptation. Robustness and resilience are closely linked but they are not identical and require partially different types of actions and instruments.

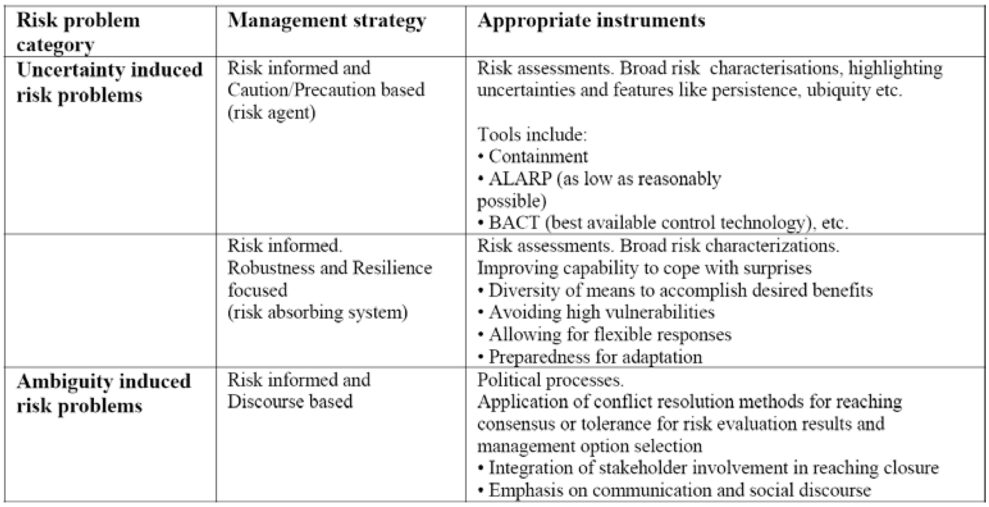
Table 1 shows the risk management implications of the risk problem categories (Renn 2005, Aven and Renn 2008b). Here *uncertainty* refers to the difficulty of predicting the occurrence of events and/or their consequences based on incomplete or invalid data bases, possible changes of the causal chains and their context conditions, extrapolation methods when making inferences from experimental results, modelling inaccuracies or variations in expert judgments. Uncertainty may result from an incomplete or inadequate reduction of complexity, and it often leads to expert dissent about the risk characterisation. Examples of high uncertainty include many natural disasters (such as earthquakes), possible health effects of mass pollutants, acts of violence such as terrorism and sabotage and long term effects of introducing genetically modified species into the natural environment. For terrorism risk, the consequences of an attack can be fairly accurately predicted. However, the time and type of attack is subject to large uncertainties.

The uncertainty may be a result of “known uncertainties” – we know what we do not know, and “unknown uncertainties” (ignorance or non-knowledge) - we do not know what we do not know. The difficulty of predicting the occurrence of events and/or their consequences depend on the models available. If variations in populations are known (for example the proportion of persons suffering a disease), the corresponding probability distributions represent a basis for accurate predictions. Variation in populations is often referred to as stochastic or aleatory uncertainties. In general, the uncertainties can be reduced by improving our knowledge and improving our models. Yet aleatory uncertainty remains fuzzy about the time, the exact location and/or the persons who will suffer.

Ambiguity refers to different views related to

i. the relevance, meaning and implications of the basis for the decision making (interpretative ambiguity); or
ii. the values to be protected and the priorities to be made (normative ambiguity).

What does it mean, for example, if neuronal activities in the human brain are intensified when subjects are exposed to electromagnetic radiation? Can this be interpreted as an adverse effect or is it just a bodily response without any health implication? Examples for high interpretative ambiguity include low dose radiation (ionising and non-ionising), low concentrations of genotoxic substances, food supplements and hormone treatment of cattle. Normative ambiguities can be associated, for example, with passive smoking, nuclear power, pre-natal genetic screening and genetically modified food.



Risk problem category	Management strategy	Appropriate instruments
Uncertainty induced risk problems	Risk informed and Caution/Precaution based (risk agent)	Risk assessments. Broad risk characterisations, highlighting uncertainties and features like persistence, ubiquity etc. Tools include: • Containment • ALARP (as low as reasonably possible) • BACT (best available control technology), etc.
	Risk informed. Robustness and Resilience focused (risk absorbing system)	Risk assessments. Broad risk characterizations. Improving capability to cope with surprises • Diversity of means to accomplish desired benefits • Avoiding high vulnerabilities • Allowing for flexible responses • Preparedness for adaptation
Ambiguity induced risk problems	Risk informed and Discourse based	Political processes. Application of conflict resolution methods for reaching consensus or tolerance for risk evaluation results and management option selection • Integration of stakeholder involvement in reaching closure • Emphasis on communication and social discourse

Table 1: Risk problem categorisations and their implications for risk management (adapted from Renn (2005))

We compare alternatives by looking at the risk picture for the various alternatives. If the alternatives are about the same with respect to other concerns, such as costs, the risk analysis gives a good basis for recommending a particular alternative. Normally, we must, however, undertake a weighing between various concerns, and then the cost-effectiveness analysis and the cost-benefit analysis come into play. In a cost-benefit analysis, we calculate the expected net present value, whereas these analyses make it possible to compare the various concerns, such as risk and costs. These analyses do not, however, provide answers to what is the correct solution and the best alternative. As is the case for all types of analysis, these analyses have their limitations and weaknesses, and they can only provide a basis for making a good decision.

The main problem of the cost-benefit analysis is related to the transformation of non-economic consequences to monetary values. What is the value of future generations? How should we determine a "correct" discount rate? The value of safety and security is not adequately taken into account by the approach. Investments in safety and security are justified by risk and uncertainty reductions, but cost-benefit analyses to a large extent ignore these risks and uncertainties. A cost-benefit analysis calculating expected net present values does not take into account the risks (uncertainties).

To explain this in more detail, consider the following example.

> In an industry, two risk reducing measures I and II, are considered. For measure I (II) the computed expected reduced number of fatalities equals 1 (2). The costs are identical for the two measures. Hence the cost-benefit approach would guide the decision maker to give priority to measure II. But suppose that there are large uncertainties about the phenomena and processes that could lead to fatalities. Say for example that measure II is based on new technology. Would that change the conclusion of the cost-benefit analysis? No, because this analysis restricts attention to the expected value. We conclude that there is a need for seeing beyond the expected value calculations and the cost-benefit analysis when determining the best alternative.

The practice of using traditional cost-benefit analyses and cost effectiveness analyses to support investments into safety and in particular to verify ALARP, has been questioned (Aven and Abrahamsen 2007). The ALARP principle is an example of application of the cautionary principle. Uncertainty should be given strong weight, and the grossly disproportionate criterion is a way of making the principle operational. However, cost-benefit analyses calculating expected net present values ignore uncertainties and the use of this approach to evaluate safety investments is therefore meaningless. The same applies to the cost effectiveness indices such as the expected cost per expected number of saved lives (referred to as the implied cost of averting a statistical fatality, ICAF) which are often used instead of full cost-benefit analyses. If a measure costs 2 million euros and the risk analysis shows that the measure will bring about a reduction in the number of expected fatalities by 0.1, then the ICAF is equal to 2/0.1 = 20 million euros. By comparing this number with reference values, we can express the effectiveness of the measure.

Modifications of the traditional cost-benefit analysis are suggested to cope with this problem, see e.g. Aven and Flage (2008). In these methods, adjustments are made to either the discount rate or the contribution from the cash flows. This latter case could be based on the use of certainty equivalents for the uncertain cash flows. Although arguments are provided to support these methods, their rationale can be questioned. There is a significant element of arbitrariness associated with this approach.

Conclusions are often self-evident when computing indices such as the expected cost per expected life saved, or expected cost per expected reduced ton of oil, over the life cycle of a project. For example, a strategy may be that measures will be implemented if the expected cost per expected life saved is less than 10 million euros.

A potential strategy for the assessment of a measure, if the analysis based on expected present value or expected cost per expected number of lives saved has not produced any clear recommendation, can be that the measure be implemented if several of the following questions give a yes-answer:

- A relatively high personnel risk or environmental risk?
- Considerable uncertainty (related to phenomena, consequences, conditions) and measure will reduce the uncertainties?
- The measure significantly increases manageability?
- High competence among the personnel can give increased assurance that satisfactory outcomes will be reached, for example fewer leakages
- Is the measure contributing to obtaining a more robust solution?
- Is the measure based on best available technology (BAT)?
- Are there unsolved problem areas personal safety-related and/or work environment related?
- Are there possible areas where there is conflict between these two aspects?
- Strategic considerations?

7. Conclusions

The traditional quantitative risk analyses provide a rather narrow risk picture, through calculated probabilities and expected values. We conclude that this approach should be used with care, in particular for problems with large uncertainties. Alternative approaches highlighting the qualitative aspects are more appropriate in such cases. A "broad" risk description is required. This is also the case when there are different views related to the values to be protected and the priorities to be made. The main concern is the value judgments, but they should be supported by solid scientific analyses, also showing a broad risk picture. If one tries to demonstrate that it is rational to accept risk, on a scientific basis, a too narrow approach to risk has been adopted. Recognizing uncertainty as a main component of risk is essential to "successfully" implement risk management.

When various alternatives are to be compared and a decision is to be made, the analysis and assessments that have been conducted provide a basis for such a decision. In many cases, established design principles and standards also provide clear guidance. Compliance with such principles and standards will be among the first reference points when assessing risks.

It is common thinking that risk management processes, and especially ALARP processes, require formal guidelines or criteria (e.g. risk acceptance criteria and cost-effectiveness indices) to simplify the decision-making. Care has however to be shown when using this type of formal decision-making criteria, as they easily result in a mechanization of the decision making process. Such a mechanisation is unfortunate because:

- Decision-making criteria based on risk-related numbers (probabilities and expected values) alone do not capture all the aspects of risk, costs and benefits.
- No method has a precision that justifies a mechanical decision based on whether the result is over or below a numerical criterion
- It is a managerial responsibility to make decisions under uncertainty, and management should be aware of the relevant risks and uncertainties.

References

Ale, B., Bellamy, L.J., van der Boom, R., Cooper, J., Cooke, R.M., Goossens, L.H.J., Hale, A.R, Kurowicka, D., Morales, O., Roelen, A.L.C. and Spouge, J. (2008) Further development of a Causal model for Air Transport Safety (CATS): Building the mathematical heart. Reliability Engineering and System Safety. To appear.

Apostolakis, G.E. and Lemon, D.M. (2005) A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism. Risk Analysis, 24(2), 361-376.

Aven, T. (2003) Foundations of Risk Analysis. New York: John Wiley \& Sons Ltd.

Aven, T. (2006) On the precautionary principle, in the context of different perspectives on risk. Risk Management: an International Journal, 8: 192-205.

Aven T. (2007a) A unified framework for risk and vulnerability analysis and management covering both safety and security. Reliability Engineering and System Safety, 92, 745-754.

Aven, T. (2008a) A semi-quantitative approach to risk analysis, as an alternative to QRAs. Reliability Engineering and System Safety, 93, 768–775.

Aven, T. (2008b) Risk Analysis. Wiley, N.J.

Aven, T. and Abrahamsen, E.B. (2007) On the use of cost-benefit analysis in ALARP processes. I. J. of Performability. 3, 345-353.

Aven, T. and Flage, R. (2008) Use of decision criteria based on expected values to support decision-making in a production assurance and safety setting. Reliability Engineering and System Safety. To appear. Aven, T. and Knudsen, B. (2008) Reliability and validity of risk analysis. Submitted for publication.

Aven, T. and Renn, O. (2008a) On risk defined as an event where the outcome is uncertain. J. Risk Research, to appear.

Aven, T. and Renn, O. (2008b) The role of quantitative risk assessments for characterizing risk and uncertainty and delineating appropriate risk management options, with special emphasis on terrorism risk. Risk Analysis, to appear.Aven, T. and Vinnem, J.E. (2007) Risk Management, with Applications from the Offshore Oil and Gas Industry. Springer Verlag, N.Y.

Cabinet Office (2002) Risk: Improving government's capability to handle risk and uncertainty. Strategy Unit Report.

Campbell, S. (2005) Determining overall risk. J. of Risk Research, 8, 569-581.

Douglas, E.J. (1983) Managerial Economics: Theory, Practice and Problems, 2nd ed. Prentice Hall, Englewood cliffs NJ.

Duijm, N.J. and Goossens, L. (2006) Quantifying the influence of safety management on the reliability of safety barriers. Journal of Hazardous Materials. 130(3): 284-292.

Fischhoff, B., Lichtenstein, S., Slovic, P., Derby, S. and Keeney. R. (1981) Acceptable Risk. Cambridge University Press, Cambridge.

Garrick, B.J. et.al. (2004) Confronting the risks of terrorism: making the right decisions. Reliability Engineering and System Safety, 86, 129-176.

Graham, J.D. and Weiner, J.B. (eds) (1995) Risk versus Risk: tradeoffs I Protecting Health and the Environment, Cambridge: Harvard University Press.

Guikema, S.D. (2007) Modeling Intelligent Actors in Reliability Analysis: An Overview of the State of the Art, in Bier, V.M. and N. Azaiez, Eds. Combining Reliability and Game Theory, Springer Series on Reliability Engineering. In press.

Guikema, S.D. and Aven, T. (2007) Assessing Risk from Intelligent Attacks: A Perspective on Approaches. Submitted for publication.

Haimes, Y.Y. (2004) Risk Modelling, Assessment, and Management, 2nd ed. Wiley, N.Y.

Hollnagel, E. (2004) Barriers and Accident Prevention, Ashgate Publishers, Aldershot.

HSE (2001) Reducing risk, protecting people. HES Books, ISBN 0 71762151 0.

ISO (2002) Risk management vocabulary. ISO/IEC Guide 73.

ISO (2005b) Risk management. General guidelines for principles and implementation of RM.

Kaplan, S. and Garrick, B.J. (1981) On the quantitative definition of risk. Risk Analysis, 1: 11-27.

Kaplan, S. (1991) Risk Assessment and Risk Management - Basic Concepts and Terminology. In Risk Management: Expanding Horizons in Nuclear Power and Other Industries, Hemisphere Publ. Corp., Boston, MA, 11-28.

Kierans, L et al (2007) Overview of approaches to accident risk evaluation (Norway), Proactima produced for Räddningsverket

Knight, F. H. (1921) Risk, Uncertainty and Profit. BoardBooks, Washington, DC. Reprinted 2002.

Léger A., Duval C., Farret R., Weber P., Levrat E. and Iung, B. (2008) Modeling of human and organizational impacts for system risk analyses. In Conference proceedings PSAM 9, Hong Kong, 19-23/5-08.

Leveson, N. (2007) Modeling and Analyzing Risk in Complex Socio-Technical Systems. NeTWork workshop, Berlin 27-29 Sept. 2007.

Levy, H. and Sarnat, M. (1990) Capital investment and financial decisions. Fourth edition. New York: Prentice Hall.

Lowrance, W. (1976) Of Acceptable Risk - Science and the Determination of Safety. William Kaufmann Inc., Los Altos, CA.

Luxhøj, J.T., A. Choopavang, and D.N. Arendt (2001), Risk Assessment of Organizational Factors in Aviation Systems, Air Traffic Control Quarterly, Vol. 9, No. 3, pp. 135-174.

Löfstedt, R. E. (2003) The Precautionary Principle: Risk, Regulation and Politics. Trans IchemE, 81, 36-43.

Mohaghegh, Z., Kazemi, R. and Mosleh, A. (2008) A Hybrid Technique for Organizational Safety Risk Analysis. In Conference proceedings PSAM 9, Hong Kong, 19-23/5-08.

Papazoglou, I.A., Bellamy, L.J., Hale, A.R., Aneziris, O.N., Post, J.G. and Oh, J.I.H. (2003) IRisk: development of an integrated technical and Management risk methodology for chemical installations. Journal of Loss Prevention in the process industries, 16, 575 - 591.

Paté-Cornell E.M. and Murphy D.M. (1996) Human and management factors in probabilistic risk analysis: the SAM approach and observations from recent applications. Reliability Engineering and System Safety, 53, 115-126.

PSA (2001) Regulations Petroleum Safety Authority Norway.

Rasmussen, J. (1997) Risk management in a dynamic society: a modelling problem. Safety Science 27 (2/ 3), 183–213.

Renn, O. (2005) Risk Governance: Towards an Integrative Approach. White Paper No. 1, written by Ortwin Renn with an Annex by Peter Graham (International Risk Governance Council: Geneva 2005)

Rosa, E.A. (1998) Metatheoretical Foundations for Post-Normal Risk, Journal of Risk Research, 1, 15-44.

Røed, W., Mosleh, A., Vinnem, J.E. and Aven, T. (2008) On the Use of Hybrid Causal Logic Method in Offshore Risk Analysis. Reliability Engineering and System Safety. To appear.

Sandin, P. (1999) Dimensions of the precautionary principle. Human and Ecological Risk Assessment, 5, 889-907.

Taleb, N. N. (2007) The Black Swan: The Impact of the Highly Improbable, London: Penguin.

Willis, H.H. (2007) Guiding resource allocations based on terrorism risk. Risk Analysis 27(3) 597-606.

Bibliography

AS/NZS 4360 (2004) Australian/New Zealand Standard: Risk management.

Aven, T. (2004) Risk analysis and science. Int. J. of Reliability, Quality and Safety Engineering, 11, 1-15.

Aven, T. (2007b) On the ethical justification for the use of risk acceptance criteria. Risk Analysis, 27, 303-312.

Aven, T., Hauge, S. Sklet, S. and Vinnem, J.E. (2006) Methodology for incorporating human and organizational factors in risk analyses for offshore installations, Int. J. of Materials & Structural Reliability, 4, 1-14.

Aven, T. and Kristensen, V. (2005) Perspectives on risk - Review and discussion of the basis for establishing a unified and holistic approach. Reliability Engineering and System Safety, 90, 1-14.

Aven, T. and Kristensen, V. (2005) Perspectives on risk - Review and discussion of the basis for establishing a unified and holistic approach. Reliability Engineering and System Safety, 90, 1-14.

Aven, T., Nilsen, E. and Nilsen, T. (2004) Economic risk - review and presentation of a unifying approach. Risk Analysis, 24, 989-1006.

Aven, T., Røed, W. and Wiencke, H.S. (2008) Risk Analysis. The University Press, Oslo (In Norwegian).

Aven, T. and Vinnem, J.E. (2005) On the use of risk acceptance criteria in the offshore oil and gas industry. Reliability Engineering and System Safety, 90, 15-24.

Aven, T., Vinnem, J.E. and Wiencke, H.S. (2007) A decision framework for risk management. Reliability Engineering and System Safety, 92, 433-448.

Bedford, T. and Cooke, R. (2001) Probabilistic Risk Analysis. Foundations and Methods. Cambridge: Cambridge University Publishing Ltd.

Clemen, R.T. (1996) Making Hard Decisions. 2nd ed. Duxbury Press, N.Y.

HSE (2003) Guidance on ALARP for offshore division inspectors making an ALARP demonstration. 1/10-03.

IEC 61511 Functional safety: safety instrumented system for the process industry sector, part 1-3, December 2003.

Jones-Lee, M. W. (1989) The Economics of Safety and Physical Risk. Basil Blackwell, Oxford, UK.

Kahneman, D. and Tversky, A. (1979) Prospect Theory: An Analysis of Decision under Risk, Econometrica, XLVII, 263-291.

Kristensen, V., Aven, T. and Ford, D. (2006) A new perspective on Renn & Klinke's approach to risk evaluation and risk management. Reliability Engineering and System Safety, 91, 421- 432.

Leva M.C. et al. (2006) SAFEDOR: A practical approach to model the action of an officer of the watch in collision scenarios. ESREL 2006.

Leveson, N. (2004) A new accident model for engineering safer systems. Safety Science, 42, 237-270.

Lindley, D. V. (1985) Making Decisions. London: John Wiley & Sons Ltd.

Modarres, M. (1993) What Every Engineer should Know about Risk. Marcel Dekker, N.Y.

Renn, O. and Klinke, A. (2002) A New approach to risk evaluation and management: Riskbased precaution-based and discourse-based strategies. Risk Analysis, 22, 1071-1094.

Renn, O. (1992) Concepts of Risk: A Classification, in: S. Krimsky and D. Golding (eds.): Social Theories of Risk. (Praeger: Westport), pp. 53-79.

Renn, O. (2007) Risk Governance. Earthscan. London 2007

RESS (2007) Reliability Engineering and System Safety 92, Issue 6. Special issue on critical infrastructures.

Sandøy, M., Aven, T. and Ford, D. (2005) On integrating risk perspectives in project management. Risk Management: an International Journal, 7, 7-21.

Singpurwalla, N. (2006) Reliability and Risk. A Bayesian Perspective. Wiley, N.Y.

van der Borst, M. and Schoonakker, H. (2001) An overview of PSA importance measures. Reliability Engineering and System Safety 72, 241-245.

Vatn, J. (2007) Societal Security - A case study related to a cash depot. Proceedings ESREL 2007.

Vinnem, J.E., Kristiansen, V. Witsø, E. (2006b). Use of ALARP evaluations and risk acceptance criteria for risk informed decision-making in the Norwegian offshore petroleum industry. Proceedings ESREL 2006.

Vose, D. (2000) Risk Analysis, A Practical Guide. Wiley, N.Y.

Watson, S.R. and Buede, D.M. (1987) Decision Synthesis. Cambridge University Press. N.Y.

Wiencke, HS, Aven, T. Hagen, J. (2006) A framework for selection of methodology for risk and vulnerability assessments of infrastructures depending on ICT. ESREL 2006, pp. 2297-2304.

Swedish Rescue Services Agency, S-651 80 Karlstad, Sweden
Telephone +46 54 13 50 00, Fax +46 54 13 56 00

Order number P21-497/08. Fax +46 54 13 56 05
ISBN 978-91-7253-425-4