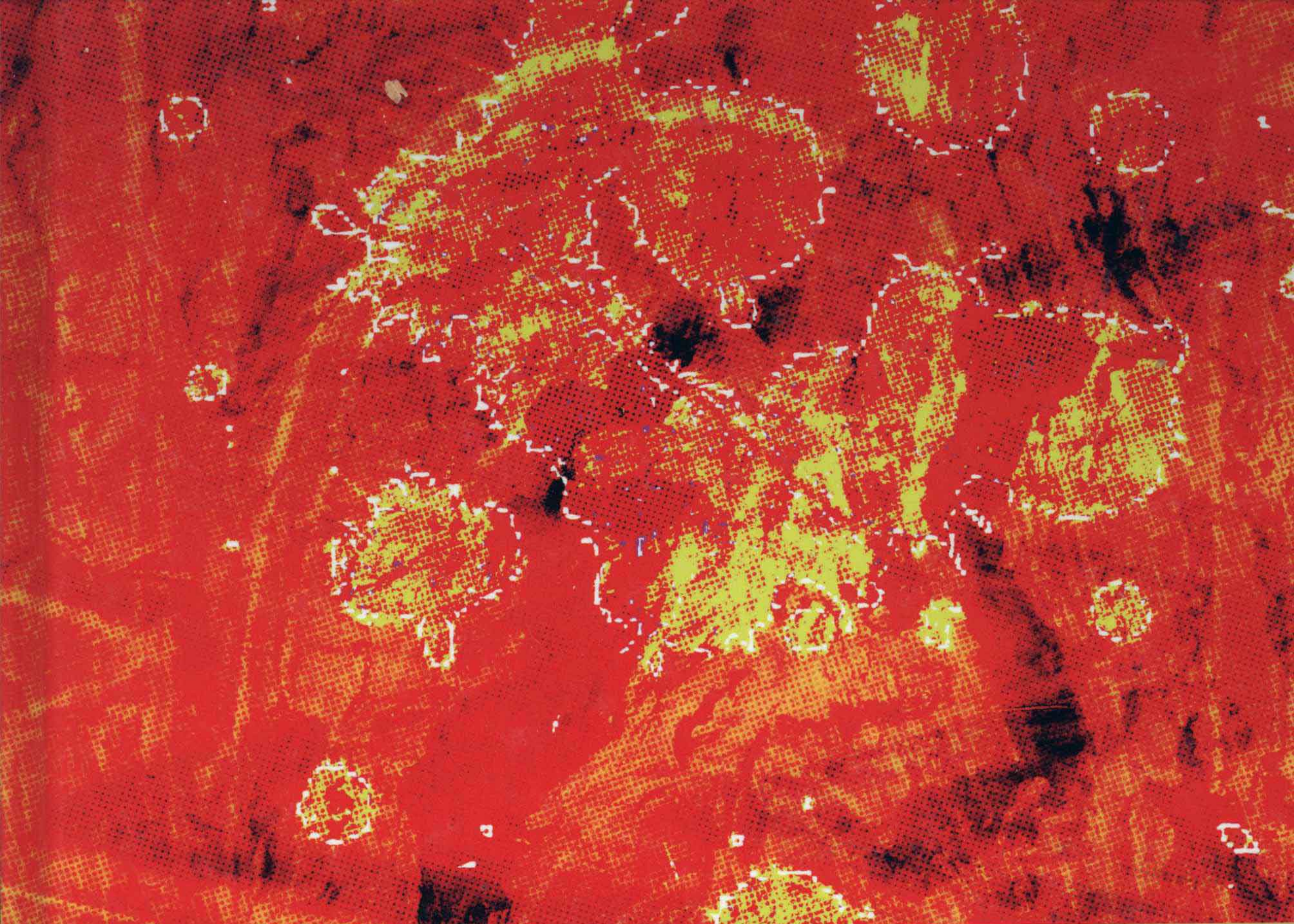

QUANTITATIVE RISK ASSESSMENT

The Scientific Platform

TERJE AVEN

CAMBRIDGE

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town,
Singapore, São Paulo, Delhi, Tokyo, Mexico City

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521760577

First published 2011

Printed in the United Kingdom at the University Press, Cambridge

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing-in-Publication Data

Aven, T. (Terje)
Quantitative risk assessment : the scientific platform / Terje Aven.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-521-76057-7 (Hardback)
1. Probabilities. 2. Risk assessment–Statistical methods.
3. Decision making–Statistical methods. I. Title.
QA273.A93 2011
519.2′87–dc22

2010037661

ISBN 978-0-521-76057-7 Hardback

Preface

Risk assessment is in many respects acknowledged as a scientific discipline per se: there are many master and PhD programmes worldwide covering this field, and many scientific journals and conferences highlighting the area. However, there are few books addressing the scientific basis of this discipline, which is unfortunate as the area of risk assessment is growing rapidly and there is an enormous drive and enthusiasm to implement risk assessment methods in organisations. Without a proper basis, risk assessment would fail as a scientific method or activity. Consider the following example, a statement from an experienced risk assessment team about uncertainty in quantitative risk assessments (Aven, 2008a):

> The assessments 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 assessment, from the hazard identification to the models and probability calculations. It is concluded that the precision of the assessment is limited, and that one must take this into consideration when comparing the results with the risk acceptance criteria and tolerability limits.

Based on such a statement, one may question what the scientific basis of the risk assessment is. Everything is uncertain, but is not risk assessment performed to assess the uncertainties? From the cited statement it looks like the risk assessment generates uncertainty. In any event, does this acknowledgment – that a considerable amount of uncertainty exists – affect the analyses and the conclusions? Only very rarely! My impression is that one writes such statements just to meet a requirement, and then they are put aside. This says a lot about the scientific quality of the assessments.

I strongly believe that the scientific platform of risk assessment – and quantitative risk assessment in particular – needs to be strengthened. The aim of this book is to contribute to this end. For many years I have been engaged in research trying to improve the scientific basis of risk assessment; I have written many books and papers related to the topic, and believe that the time has come to publish a fundamental exposition on the topic *quantitative risk assessment – the scientific platform*. The basic idea is to provide a framework for analysing and discussing the quality of the assessments using the scientific requirements of reliability and validity. The reliability requirement is concerned with the consistency of the "measuring instrument" (analysts, experts, methods, procedures), whereas validity is concerned with the assessment's success at "measuring" what one set out to "measure". This gives a new and original approach to the analysis and discussion.

The quality of risk assessment relates to the scientific building blocks of the assessments but also to the role of the assessments in the decision-making process. On an overall level one can say that the purpose of risk assessment is to support the decision-making – to adequately inform the decision-makers – but what type of decision support (knowledge, judgements) should the assessments provide? Are the objectives (expectations) accurate risk estimates and/or uncertainty characterisations (representations/expressions of the knowledge and lack of knowledge available)? The scientific quality of the assessments obviously needs to be seen in relation to these objectives. Also the requirements of reliability and validity depend on these objectives. Using these criteria, we can evaluate the quality of the assessments for different objectives of the assessments.

Uncertainty is a key topic when discussing the scientific platform of risk assessment. Other important issues are the meaning of a probability, the use of Bayesian ideas and concepts, the meaning of risk, how risk should be described, the meaning and use of models, model uncertainty, the meaning and use of probability models and parameters, and the value of information.

The book is general and is relevant for all types of applications, but safety engineering has the main focus.

For many years there has been a lively discussion about the scientific platform of statistical analysis in general: the Bayesian/non-Bayesian controversy; see e.g. Lindley (2000). However, there has not been much work on establishing a proper scientific basis for risk assessments. A number of papers address foundational issues of risk assessment; see e.g. Apostolakis (1988, 1990), Kaplan and Garrick (1981), Singpurwalla (1988, 2006) and Cooke (1991), but I am not aware of much work where fundamental scientific quality requirements such as reliability and validity are discussed in the context of a risk assessment (Aven and Heide, 2009).

Of the few contributions found in the literature I would like to draw attention to the first issue of the international scientific journal *Risk Analysis* in 1981, and in particular Weinberg (1981) and Cumming (1981). These authors describe some of the problems of risk assessments, and express a large degree of scepticism about the scientific reliability and validity of risk assessments. Weinberg notes that "one of the most powerful methods of science – experimental observations – is inapplicable to the estimation of overall risk". Graham (1995) writes that the discipline "should (and will) always entail an element of craft-like judgment that is not definable by the norms of verifiable scientific fact", and that "any determination that a risk has been 'verified' is itself a judgment that is made on the basis of standards of proof that are to some extent arbitrary, disputable, and subjective" (Aven and Heide, 2009).

I share many of the same views on the scientific basis of risk assessment. However, in order to gain more insight into this subject and be able to make guidance on how to ensure and strengthen the scientific quality of risk assessments, we need to clarify the scientific pillars of the risk assessment and tailor the assessments to the decision-making context. As mentioned above, this is exactly what the present book does.

Small illustrating examples are included in the book for making concepts concrete and to illustrate ideas and principles. Three extended examples (case studies) will be presented early in the book (Chapter 4) and are pursued through the rest of the book. The first of these examples is related to the analysis of accident data, the second relates to the siting of a Liquefied Natural Gas (LNG) plant and the third discusses the design of a safety system. The idea is not that every concept or step of a risk assessment would be illustrated in each case study, but that these cases would recur often enough that the readers get a feel for the overall scope and shape of a real risk assessment and its use and are able to relate the scientific requirements to these concepts and steps. The cases are simplified so that the intellectual lessons are clarified, but they are nevertheless realistic.

The three cases illustrate different types of risk assessments. The first case covers a statistical data analysis, whereas the second shows an example of a system analysis which is strongly based on modelling of the phenomena studied. In Case 2 a large number of unknown quantities (model parameters) on the subsystem/component level need to be assessed. The third case presents an example of a reliability analysis of a specific system. The results of such analyses constitute important input to risk assessments.

Before we present and analyse the three main cases, we first review basic concepts and perspectives on how to define, understand and describe risk (Section 2). The aim is to give the reader an overview of the many different ways one can look at risk and to provide a structure for the coming analysis. We also discuss some fundamental issues related to science in a risk assessment context (Chapter 3): what are the basic features of risk assessment as a scientific method and how is risk assessment related to other scientific disciplines? This chapter also summarises the reliability and validity requirements mentioned above. Then in Chapters 5 and 6 we examine the three cases with respect to these scientific requirements: Chapter 5 looks at the situation when the objective of the risk assessment is accurate risk estimation, whereas Chapter 6 restricts attention to situations where the objective of the risk assessment is uncertainty characterisations. In Chapter 7 we discuss the implications of the findings in Chapters 5 and 6 for risk management and communication. Key issues addressed are the use of risk acceptance criteria, risk reduction processes, and the cautionary and precautionary principles.

From this analysis we are led to Chapter 8 which discusses and provides guidance on how risk should be approached, i.e. how we should define, understand and describe risk, as well as use risk assessments in a decision-making context. Chapter 9 provides some conclusions from the previous chapters.

The book allows for scientific analysis of different types of risk assessments, in particular assessments which in a detailed way reflect human and organisational factors. The book includes examples of assessments which reflect such factors, but it is beyond the scope of the book to provide a detailed account of these types of assessments. Well-selected references are presented for readers who do want to delve deeper in this area. See Section 1.1.

The book is for professionals in the field, as well as for graduate students and researchers. It should also be of interest to many policy makers and business people. The book would make it possible for them to better understand the boundaries of risk assessments and how they should be used for decision-making. The book is advanced (conceptually) but at the same time rather simple and easy to read. It has been a goal to avoid too many technicalities, but without diminishing the requirement for precision and accuracy. The main ideas and principles are highlighted. Readers would benefit from a basic knowledge in probability calculus and statistics as well as in risk assessment methods. It has, however, been a goal to reduce the dependency on extensive prior knowledge. The key statistical and risk concepts will be introduced and discussed thoroughly in the book. Thus the readers do not need to be experts on, for example, regression analysis. The focus will be on the basic ideas – "advanced statistical analysis" is not required. Appendix A provides a summary of basic theory (e.g. probability, Bayesian analysis). Appendix B includes a listing of some key definitions.

Acknowledgments

Many people have provided helpful comments and suggestions for this book. In particular, I would like to acknowledge Eirik B. Abrahamsen and Roger Flage for the great deal of time and effort they spent on reading and preparing comments on earlier versions of the book. I would also acknowledge Jan Terje Kvaløy for his kind help in producing the probability distribution shown in Figure 6.2. I am also grateful to two anonymous reviewers for valuable comments and suggestions on the plans for the book.

This work has been funded by The Research Council of Norway through the SAMRISK and PETROMAKS research programmes. The financial support is gratefully acknowledged.

I also acknowledge the editing and production staff at Cambridge University Press for their careful and effective work.

Contents

1

Introduction to risk management and risk assessments. Challenges

This chapter provides a broad introduction to risk management and risk asssessment, as a basis for the analyses and dicussions in the coming chapters. The presentation highlights general features but also challenges related to the definitions and use of these tools. Key references for the chapters are Bedford and Cooke (2001), Vose (2008) and Aven and Vinnem (2007). The terminology is to a large extent in line with ISO (2009a). See summary of key definitions in Appendix B.

1.1 General features of risk management and risk assessments

Risk management is all coordinated activities to direct and control an organisation with regard to risk. Two main purposes of the risk management are to ensure that adequate measures are taken to protect people, the environment and assets from undesirable consequences of the activities being undertaken, and to balance different concerns, for example safety and costs. Risk management covers both measures to avoid the occurrence of hazards/threats and measures to reduce their potential consequences. In industries like nuclear and oil & gas, risk management was traditionally based on a prescriptive regulating regime, in which detailed requirements for the design and operation of the plant were specified (Kumamoto, 2007; Aven and Vinnem, 2007). This regime has gradually been replaced by more goal-oriented regimes, putting emphasis on what to achieve rather than on the means of doing so. Goal orientation and risk characterisations are two major components of these new regimes that have been enthusiastically endorsed by international organisations and various industries (see e.g. IAEA Guidelines (1995), HSE (2001), Kröger (2006); the IPCS and WHO risk terminology document (2004) and the risk management guidelines of the EU Commission (European Commission, 2000, 2003; IEC, 1993)). Such an approach to risk management is believed to provide higher levels of performance both in terms of productivity and risk reduction (Aven and Renn, 2009b).

Quantitative risk assessment

Quantitative Risk Assessment (QRA) (also referred to as Probabilistic Risk Assessment – PRA) is a key tool used in these new approaches. A QRA systemises the present state of knowledge including the uncertainties about the phenomena, processes, activities and systems being analysed. It identifies possible hazards/threats (such as a gas leakage or a fire), analyses their causes and consequences, and describes risk. A QRA provides a basis for characterising the likely impacts of the activity studied, for evaluating whether risk is tolerable or acceptable and for choosing the most effective and efficient risk policy, for example with respect to risk-reducing measures. It allows for the calculation of expected values so that different risks can be directly compared. Common practice in probabilistic risk assessment avoids, however, the aggregation of the two components and leaves it to the risk evaluation or management team to draw the necessary conclusions from the juxtaposition of loss and probabilities (Aven, 2003; Kröger, 2005). In addition, second-order uncertainties are introduced via different types of uncertainty intervals to make the confidence of probability judgements more explicit (Apostolakis and Pickett, 1998; Aven, 2003), see also Sections 2.7 and 8.3. For some extensive reviews of the use of QRA/PRA in a historical perspective, see Rechard (1999, 2000).

Some of the basic tools used for analysing the probabilities and risk are statistical estimation theory, fault tree analysis (FTA) and event tree analysis (ETA). These tools belong to the following main categories of basic analysis methods:

(a) *Statistical methods:* Data are available to predict the future performance of the activity or system analysed. These methods can be based on data extrapolation or probabilistic modelling.
(b) *Systems analysis methods:* These methods (which include FTA and ETA) are used to analyse systems where there is a lack of data to accurately predict the future performance of the system. Insights are obtained by decomposing the system into subsystems/components for which more information is available. Overall probabilities and risk are a function of the system's architecture and of the probabilities on the subsystems/component level (Paté-Cornell and Dillon, 2001).

Quantitative risk assessment (QRA) is often associated with system analysis methods (see e.g. Bedford and Cooke, 2001), but in this book we interpret QRA (PRA) as any risk assessment which is based on quantification of risk using probabilities.

A number of new and improved methods have been developed in recent years to better meet the needs of the analysis, in light of the increasing complexity of the systems and to respond to the introduction of new technological systems (Aven and Zio, 2011). Many of the methods introduced allow for increased levels of detail and precision in the modelling of phenomena and processes within an integrated framework of analysis covering physical phenomena, human and organisational factors as well as software dynamics (e.g. Mohaghegh *et al.*, 2009; Luxhoj *et al.*, 2001; Ale *et al.*, 2009; Røed *et al.*, 2009). Other methods are devoted to the improved representation and analysis of the risk and related uncertainties, in view of the decision-making tasks that the outcomes of the analysis are intended to support. Examples of relatively newly introduced methods are Bayesian Belief Networks (BBNs), Binary Digit Diagrams (BDDs), multi-state reliability analysis, Petri Nets and advanced Monte Carlo simulation tools. For a summary and discussion of some of these models and techniques, see Bedford and Cooke (2001) and Zio (2009).

The traditional risk assessment approach used in QRAs 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 (e.g. Rasmussen, 1997; Hollnagel, 2004; Leveson, 2004). It is argued that some of the key methods used in risk assessments 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 for example in 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.

Leveson (2004) 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 Modeling and Processes).

Nonetheless, the causal chains and event modelling approach has shown to work for a number of industries and settings. It is not difficult to point at limitations of this approach, but the suitability of a model always has to be judged with reference to not only 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. Furthermore, the causal chains and event modelling approach is continuously improved, incorporating human, operational and organisational factors, as was mentioned above. Mohaghegh *et al.* (2009), for example, present a "hybrid" approach for analysing dynamic effects of organisational factors on risk for complex socio-technical systems. The approach links system dynamics, Bayesian belief networks, event sequence diagrams and fault trees.

For the purpose of the present book, it suffices to consider the basic analysis tools such as fault tree and event tree models, probability models and statistical inference based on these models.

Risk assessment covers risk analysis and risk evaluation; see Figure 1.1. Risk analysis is a methodology designed to determine the nature and extent of risk. It comprises the following three main steps:

1. Identification of hazards/threats/opportunities (sources)
2. Cause and consequence analysis, including analysis of vulnerabilities
3. Risk description, using probabilities and expected values.

This definition of risk analysis seems to be the most common, but there are others (refer to IRGC, 2005). One of these considers risk analysis as an overall concept, comprising risk assessment, risk perception, risk management, risk communication, and their interactions. This interpretation has been often used among members of the Society of Risk Analysis.

Expressing risk also means to perform sensitivity analyses. The purpose of these analyses is to show how sensitive the output risk indices are with respect to changes in basic input quantities, assumptions and suppositions.

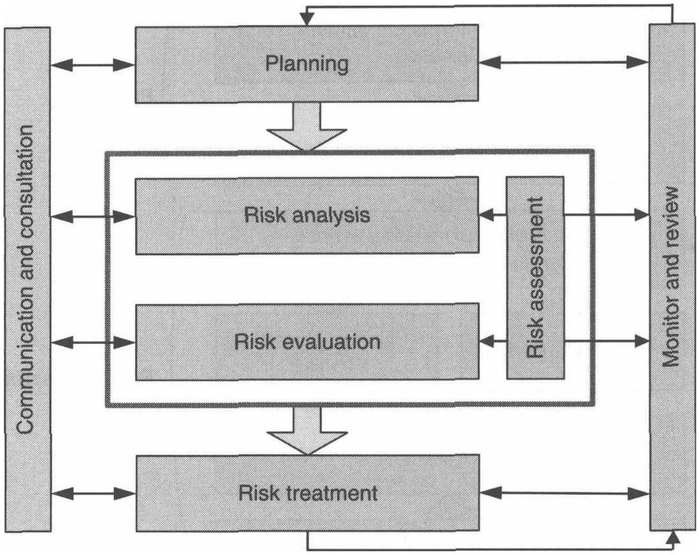

Figure 1.1 The risk assessment process (based on ISO, 2009b). Note that the ISO (2009a,b) does not include source identification as a part of risk analysis.

The sensitivity analyses can be used to identify critical systems, and thus provide a basis for selecting appropriate measures. To illustrate this, let R be a risk index, for example expressing the expected number of fatalities or the probability of a system failure, and let R_i be the risk index when subsystem i is in the functioning state. Then a common way of ranking the different subsystems is to compute the risk improvement potential (also referred to as the risk achievement worth) $I_i = R_i - R$, i.e. the maximum potential risk improvement that can be obtained by improving system i. The potential I_i is referred to as a risk importance measure. See Aven and Nøkland (2010) for a recent review of such measures.

Having established a risk description (risk picture), its significance is then evaluated (risk evaluation). Is the risk high compared to relevant reference values or decision criteria? How does alternative A compare with alternative B? etc. Risk analysis is often used in combination with risk acceptance criteria, as inputs to risk evaluation. Sometimes the term "risk tolerability limits" is used instead of risk acceptance criteria. The criteria state what is deemed as an unacceptable risk level. The need for risk-reducing measures is assessed with reference to these criteria. In some industries and countries, it is a requirement in regulations that such criteria should be defined in advance of performing the analyses.

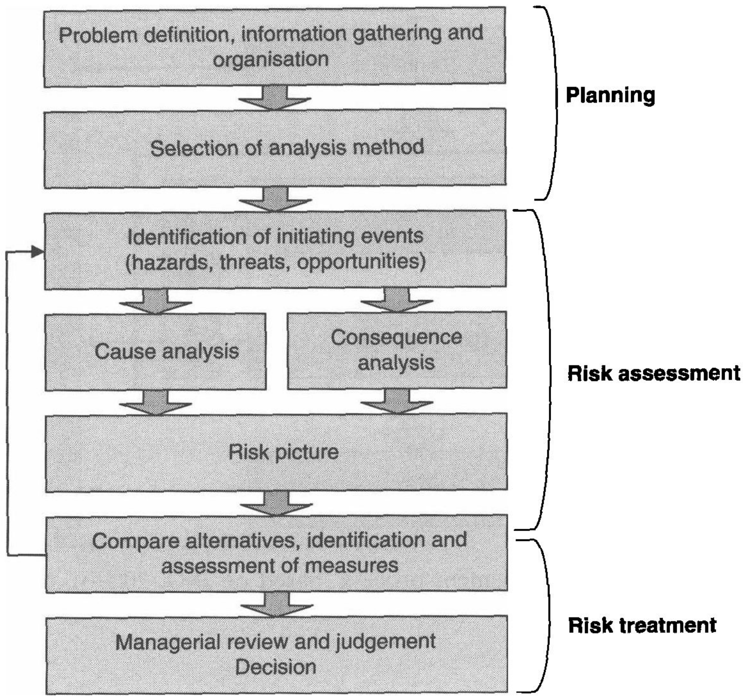

Figure 1.2 The main steps of the risk assessment process, covering the planning, the risk assessment and its use (based on Aven, 2008a).

The risk assessment process (planning, execution and use of 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 ("optimise"), transfer or retain risk. Risk transfer means sharing with another party the benefit or loss associated with the risk. It is typically effected through insurance.

"Planning" defines the basic frame conditions within which the risks must be managed and sets the scope for the rest of the risk assessment process. It means definition of suitable decision criteria as well as structures for how to carry out the risk assessment.

It is possible to detail the process in Figure 1.1 in many different ways to illustrate the planning, execution and use of risk analyses. Figure 1.2 shows an example based on Aven (2008a).

The results of the assessments need to be evaluated in the light of the premises, assumptions and limitations of these assessments. We refer to this stage of the process as the managerial review and judgement (Hertz and

Thomas, 1983; Aven, 2003). The assessments are based on some background knowledge that must be reviewed together with the results of the assessments. Consideration should be given to factors such as (Aven, 2003):

- which decision alternatives have been analysed
- which performance measures have been assessed
- the fact that the results of the analyses represent judgements (expert judgements)
- difficulties in assigning probabilities in the case of large uncertainties
- the fact that the assessments' results apply to models that are simplifications of the real world and real world phenomena.

The decision-making basis will seldom be in a format that provides all the answers that are important to the decision-maker. There will always be limitations in the information basis and the review and judgement described means that one views the basis in a larger context. Perhaps the analysis did not take into consideration what the various measures mean for the reputation of the enterprise, but this is obviously a condition that is of critical importance for the enterprise. The review and judgement must also cover this aspect.

The weight the decision-maker gives to the basis information provided depends on the confidence he/she has in those who developed this information. However, even if the decision-maker has maximum confidence in those doing this work, the decision still does not come about on its own. It is often difficult to make decisions when the risk is high. The decisions encompass difficult considerations and weighting with respect to uncertainties and values, and this cannot be delegated to those who create the basis information. It is the responsibility of the decision-maker to undertake such considerations and weighting, and to make a decision that balances the various concerns.

Apostolakis (2004, p. 518) makes this clear:

> I wish to make one thing very clear: QRA results are *never* the sole basis for decision-making by responsible groups. In other words, safety-related decision-making is *risk-informed*, not risk-based.

Figure 1.3 illustrates the use of risk assessment in the decision-making. Risk assessment is carried out to support the decision-making, for example a choice between various concepts, design configurations, risk-reducing measures etc. Other types of assessment are also needed, such as cost-effectiveness analyses and cost–benefit analyses.

The same types of ideas are reflected in many other decision analysis frameworks and contexts, for example the analytic-deliberative process

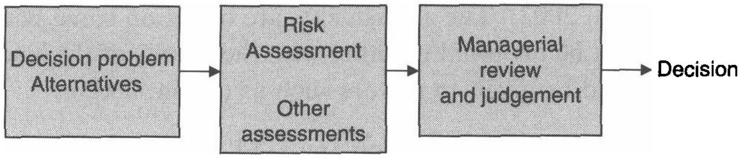

Figure 1.3 Model of the use of risk assessment to support decision-making.

recommended by the US National Research Council (1996) in environmental restoration decisions involving multiple stakeholders. According to this process, analysis "uses rigorous, replicable methods, evaluated under the agreed protocols of an expert community – such as those of disciplines in the natural, social, or decision sciences, as well as mathematics, logic, and law – to arrive at answers to factual questions"; while "deliberation is any formal or informal process for communication and collective consideration of issues. ... Participants in deliberation discuss, ponder, exchange observations and views, reflect upon information and judgements concerning matters of mutual interest and attempt to persuade each other." Such a process is particularly adapted to and relevant to decisions of great public interest.

Various decision-making strategies can form the basis for the decision. By "decision-making strategy" we mean the underlying thinking that goes on, and the principles that are to be followed with respect to how the decision is to be made, and how the process prior to the decision should be. Central to this is the question of who will be involved, how to use the various forms of analyses, and how the actual process is to be carried out.

ALARP principle

An example of such a strategy is to use risk acceptance (tolerability) criteria as inputs to risk evaluation. Another strategy is to adopt the ALARP principle, which means that risk should be reduced to a level that is as low as reasonably practicable. According to the ALARP principle, a risk-reducing measure should be implemented provided it cannot be demonstrated that the costs are grossly disproportionate relative to the gains obtained (the burden of proof is reversed). The standard approach when applying the ALARP principle, as for example used in the UK, is to consider three regions:

1. the risk is so low that it is considered negligible
2. the risk is so high that it is intolerable
3. an intermediate level where the ALARP principle applies.