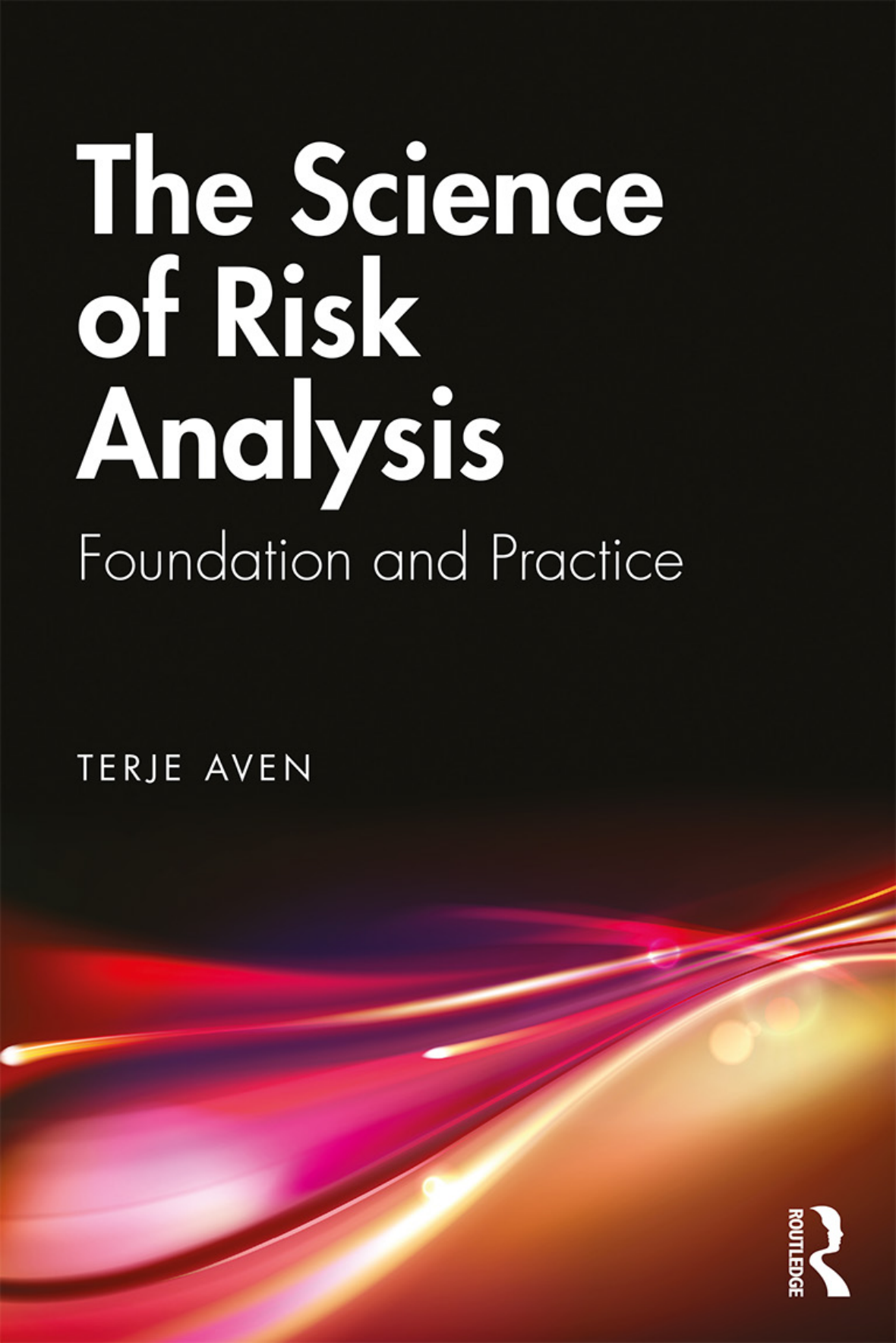
The Science of Risk Analysis

Foundation and Practice

TERJE AVEN



The Science of Risk Analysis

This book provides a comprehensive demonstration of risk analysis as a distinct science covering risk understanding, assessment, perception, communication, management, governance and policy. It presents and discusses the key pillars of this science, and provides guidance on how to conduct high-quality risk analysis.

The Science of Risk Analysis seeks to strengthen risk analysis as a field and science by summarizing and extending current work on the topic. It presents the foundation for a distinct risk field and science based on recent research, and explains the difference between applied risk analysis (to provide risk knowledge and tackle risk problems in relation to for example medicine, engineering, business or climate change) and generic risk analysis (on concepts, theories, frameworks, approaches, principles, methods and models to understand, assess, characterise, communicate, manage and govern risk). The book clarifies and describes key risk science concepts, and builds on recent foundational work conducted by the Society for Risk Analysis in order to provide new perspectives on science and risk analysis. The topics covered are accompanied by cases and examples relating to current issues throughout.

This book is essential reading for risk analysis professionals, scientists, students and practitioners, and will also be of interest to scientists and practitioners from other fields who apply risk analysis in their work.

Terje Aven is Professor of Risk Analysis and Risk Management at the University of Stavanger, Norway. He has served as the Chair of the European Safety and Reliability Association (ESRA) and as the President of the Society for Risk Analysis (SRA) worldwide. He is Editor-in-Chief of the *Journal of Risk and Reliability*, and Associate Editor for *Risk Analysis*.

The Science of Risk Analysis

Foundation and Practice

Terje Aven

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2020
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
52 Vanderbilt Avenue, New York, NY 10017

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record has been requested for this book

ISBN: 978-0-367-13919-3 (hbk)
ISBN: 978-0-367-13922-3 (pbk)
ISBN: 978-0-429-02918-9 (ebk)

Typeset in Sabon
by Swales & Willis Ltd, Exeter, Devon, UK

Contents

Preface

This book is about risk understanding, risk assessment, risk characterization, risk communication, risk management, risk governance and policy relating to risk, in the context of risks which are a concern for individuals, public and private sector organizations and society at a local, regional, national or global level. Following a long tradition of the Society for Risk Analysis (SRA 2015a), the term 'risk analysis' is used as a common term for all these aspects and activities of risk. Certainly, 'risk analysis' is not an ideal term to use for this purpose, as it also has a narrower interpretation: "the process to comprehend the nature of risk and to express the risk, with the available knowledge" (SRA 2015a). However, no suitable holistic term exists, and 'risk analysis', as used above in the broad sense, has a history of close to 40 years, supported by the international well recognized scientific journal, *Risk Analysis*.

Frequently, the 'risk field' and 'risk science' will also be referred to in the same sense as 'risk analysis'. The book argues that risk analysis is a scientific field and science. The book presents the main building blocks for this field and science. Today, risk analysis is not broadly recognized as a separate science. In my view, this fact represents a huge obstacle for the further development of risk analysis. It makes it difficult to obtain funding for research on generic topics of risk analysis and to establish educational programmes and academic positions at our universities and colleges. The total volume of research and funding, as well as the number of academic study programmes and positions in risk analysis, is rather small, if we compare it with statistics, for example. Currently, there are in fact very few specific risk analysis professors worldwide. Why should statistics have thousands of university professors working on improving the fundamentals of statistical principles, approaches and methods, whereas risk analysis has hardly any? As will be discussed below and in Chapter 3, risk analysis is in many respects similar

to statistics – it has a generic part and it is used in all types of applications to solve practical problems. Is not risk analysis important enough to justify a similar position in society?

Think about all the big challenges of the world today. Is not risk an important aspect? Risk is central to them all – to climate change, health, security and technology issues. How to generate suitable risk knowledge is at the core of risk analysis, and it is not trivial. There is a need for a science that can provide authoritative guidance on how to think in relation to this task, that challenges current procedures and searches for improvements. No other science addresses risk as such. In, for example, medicine, the main task is really to understand what causes a specific disease and how it best can be treated, not how risk should be best conceptualized and described. For risk analysis, the latter challenges are, however, key drivers. Similarly, the main driver of statistics as a science is to establish the most suitable concepts, principles and methods for collecting, analysing, presenting and interpreting data. In this way, both risk analysis and statistics support medicine and other sciences like psychology, natural sciences and engineering, but they are not and should not only be motivated by solving specific problems in specific areas. If that were the case, not much development and progress would result, as there would be limited ways of learning and building on insights from different types of problems. However, statistics and risk analysis do exactly that – the fields extend beyond the specific applications, through their generic knowledge generation on concepts, theories, frameworks, approaches, principles, methods and models.

Unfortunately, the risk analysis foundation is still rather weak. Think of a PhD student in civil engineering, who studies a risk-related topic (Aven 2018a). As his/her field is civil engineering, the thesis will be evaluated by its contribution to this field and not to that of risk analysis. The student needs to incorporate aspects of relevant risk theory and methods, but, as the civil engineering application is central, there is no drive to improve the ideas and theories from a risk analysis point of view. On the contrary, in many cases it is sufficient to use material which is considered outdated from a risk analysis field perspective. For example, the problems of seeing risk as the expected value are well known from the risk analysis literature, but this way of understanding risk is often rather uncritically used in applied work. From the applied point of view, it does not matter so much as the contribution is not to risk analysis per se but to civil engineering. This situation is not unusual, as the risk analysis area has not been able to establish a common platform guiding new applications. For scholars outside the risk analysis area, it is not easy to see the generic risk analysis developments being made. This situation is serious, as it hampers the necessary improvements within applications of risk analysis.

Similar to the PhD student, consider a talented young scholar who would like to pursue a career in risk analysis. If he/she would like to obtain a future professorship position, he/she must think about contributions in existing fields/disciplines and, with few positions in risk analysis, his/her research interests and priorities will need to be adjusted accordingly. This situation is problematic for the risk field; with few young researchers seeing risk analysis as their scientific field, there will not be enough scholars building the necessary interest and foundation for the field: scholars who can build the platform that is needed to drive risk analysis forward and balance the influence from the applied fields.

To best meet risk problems, we need a strong risk analysis field and science that can stimulate the development of suitable concepts, principles and methods. If such developments are mainly driven by applications and not a genuine interest in the risk analysis field itself, fewer and less creative advancements are foreseen. The issues raised by applications are essential for the risk analysis field, to formulate the right questions and ensure relevancy, but these need to be supplemented by researchers who see beyond the applications and find a deeper understanding and can develop improved risk analysis approaches and methods. For example, generic studies on the meaning of the risk concept could obviously provide new insights about risk to the benefit of all types of applications. Every application needs not, and should not, start from scratch when seeking to find the best concepts, principles, approaches and methods for its use. The risk analysis field should provide some 'approved' insights and guidelines that the applications can make use of.

OBJECTIVES

This book seeks to contribute to strengthening risk analysis as a field and science by summarizing and extending current work on the topic. The main objectives of the book are to provide a comprehensive demonstration of risk analysis as a science per se, present and discuss the key pillars of this science, and provide guidance on how to conduct high-quality risk analysis.

CONTENT

Chapter 1 introduces a set of cases that will be used throughout the book to illustrate ideas, concepts and principles. These cases cover, among others, climate change risk, security risks, global risks and risk governance. Situations with low probability and high impact are highlighted in this book.

Chapter 2 provides some fundamentals about science, knowledge and research. To be able to build a risk analysis field and science, we need to clarify what science means. There are different perspectives on this fundamental question, and the remaining parts of the book are strongly dependent on the pillars provided in this chapter. The basic idea is that science is to be seen as the most warranted statements – the most justified beliefs – that can be made, at the time being, on the subject covered by the relevant knowledge discipline. Understanding the concept of knowledge is thus critical and how knowledge is generated through research. It is stressed that the chapter does not provide a thorough review of the literature on science – what is covered is the necessary platform for building the risk analysis science.

Chapter 3 defines, presents and justifies the risk analysis field and science. A distinction is made between applied risk analysis and generic risk analysis. Risk analysis is discussed in relation to other sciences, including natural and social sciences. The question about risk analysis being a multidisciplinary or interdisciplinary field is also discussed.

Chapter 4 adds further details to the framework established in Chapter 3, by clarifying and discussing the risk concept and how to describe or characterize risk. The probability concept is thoroughly discussed.

The following four chapters, 5–8, look specifically into the topics of risk assessments, risk perception and communication, risk management and governance, and solving practical risk analysis problems, respectively. Using these headings, the structure established by the Society for Risk Analysis (SRA 2017a) on the core subjects of risk analysis is adopted. The aim of these four chapters is not to provide all-inclusive coverage of these subjects – that is of course not possible – but to address key issues and challenges. For instance, in the risk assessment chapter, attention is on, for example, the validity and reliability criteria, conservatism and rare events, not on how to use event trees and Bayesian networks to assess risk.

Chapter 9 provides some final remarks, with some perspectives on the future of risk analysis.

In addition, the book includes two appendices, on the terminology adopted in the book (which is mainly based on the Society for Risk Analysis Glossary, SRA 2015a) and on the core subjects of risk analysis, as defined by the SRA (2017a). Some bibliographic notes are also included.

It is possible to highlight many types of issues and examples to illustrate the key points made in this book. The present work is, to a large extent, founded on recent documents produced by the Society for Risk Analysis and related research (SRA 2015a, b, 2017a, b). This gives the book a rather broad basis, as many highly qualified scholars have been involved in the SRA work, with competence and experience from different areas of risk analysis.

However, subjectivity in the selection of papers, issues and examples for the book is acknowledged.

The aim has been to produce an authoritative, scientifically founded risk book, which gives due attention to reflections, for a rather broad readership. The main target group for the book is risk analysis scientists and professionals, but also graduate students. It should also be of interest to scholars from other fields and sciences, who apply risk analysis in their work. I also believe the book could be useful for managers, policy-makers and business people, at least parts of it, as risk is relevant in so many decision-making contexts. The book is conceptually sophisticated but, at the same time, rather easy to read. The focus is on ideas and principles, not the technicalities. For sure, readers would benefit from being familiar with basic probability theory and statistics, as well as risk assessment methods, but the book does not require much prior knowledge. The key concepts and terminology will be carefully introduced and discussed within the text.

The book is about fundamental issues in risk analysis, and it seeks to provide clear guidance in this context. However, it does not prescribe which risk analysis method or procedure should be used in different situations. No recipes are presented. What is included is the overall thinking process related to the understanding, assessment, communication, management and governance of risk.

The rather critical points made on the treatment of risk and uncertainty related to the work by the Intergovernmental Panel on Climate Change (IPCC) should not be interpreted as an expression of scepticism toward the main insights from the IPCC climate-change reports or even misjudged as taking a critical position towards the major assumption of anthropogenic climate change. This is not the author's field of expertise. The motivation for the critique is to contribute to improving the work on assessing and handling risk and uncertainties in general and related to climate change in particular.

Acknowledgments

I would like to acknowledge Ortwin Renn, Seth Guikema, Enrico Zio, Roger Flage and Eirik B. Abrahamsen, for their valuable input to this book, through their collaboration on relevant projects and papers. This book would not have been a reality without the inspiration and enthusiasm shown by these colleagues and friends. I would particularly like to thank Eirik B. Abrahamsen and Roger Flage for the time and effort they spent on reading and commenting on an earlier version of the book. Many other scholars have also contributed to the book, by taking part in the discussions of the foundation of risk analysis, including Tony Cox, Sven-Ove Hansson, Michael Greenberg, Wolfgang Kröger and Katherine McComas. Thanks to all. None of you bear any responsibility for the book content with its views and possible shortcomings.

Terje Aven
1 February 2019

1 Introduction

Challenges

This chapter presents some examples that will be frequently referred to throughout the book to illustrate the presentation and discussion. The examples demonstrate some of the fundamental problems current risk analysis practice is facing. In later chapters, the problems will be rectified using recent developments in the field and science of risk analysis.

1.1 CLIMATE CHANGE RISK: CONCEPTS AND COMMUNICATION

Few global threats rival global climate change in scale and potential consequence. The principal international authority assessing climate risk is the Intergovernmental Panel on Climate Change (IPCC). Through repeated assessments, the IPCC has devoted considerable effort and interdisciplinary competence to articulating a common characterization of climate risk and uncertainties. The IPCC aims at informing governments and decision-makers at all levels about scientific knowledge on climate change issues. Their work is, to a large extent, about risk. The communication can be viewed as successful, in the sense that most governments are now taking serious action, in line with the main conclusions made by the IPCC.

However, the scientific quality of the risk assessments and characterizations made can be questioned and, hence, also the related risk communication. Strong criticism has been raised against the way risk is dealt with in the IPCC work. For example, in their review of the assessment and its foundation for the Fifth Assessment Reports published in 2013 and 2014, Aven and Renn (2015) argue that the IPCC work falls short of providing a theoretically and conceptually convincing foundation on the treatment of risk and uncertainties. The main reasons for their conclusions are: (i) the concept of

risk is given a too narrow understanding, and (ii) the reports lack precision in delineating their concepts and methods.

The panel seems to have developed its approach from scratch without really consulting the scientific community and literature on risk analysis. For the IPCC, this community and literature have clearly not provided the authoritative guidance that could support it in forming its approach to risk. This demonstrates that the field and science of risk analysis is too weak to have an impact on important scientific work such as climate change research. The result is a poor IPCC conceptualization and treatment of risk and uncertainties.

For example, to characterize risk the IPCC uses the likelihood/probability concept, but an understandable interpretation is not provided. The IPCC states for instance that it is extremely likely – at least 95 per cent probability – that most of the global warming trend is a result of human activities (IPCC 2014a), without expressing what this important statement means; refer to Section 6.2.1.

In the 2007 IPCC reports (IPCC 2007, p. 64), risk was generally understood to be the product of the likelihood of an event and its consequences (the expected value), but this interpretation of risk is not used in the latest reports. The concept of expected values representing risk in situations such as climate change has proved to be inadequate, as emphasized by many analysts and researchers (Haimes 2015, Paté-Cornell 1999 and Aven 2012a); see also Chapter 4.

In later IPCC documents – see for example the Guidance note from 2010 (IPCC 2010) – this understanding of risk is replaced by a perspective where risk is a function of likelihood (probability) and consequences. However, strong arguments can be provided – see Chapter 4 – that this risk perspective is also inadequate for assessing climate change risk. The concept of risk in the IPCC works refers to likelihood/probability, but, with no interpretation of this concept, the concept of risk also becomes undefined and vague. Equally important, significant aspects of risk are not really incorporated, as will be thoroughly discussed in Chapter 4, see also Section 6.2.1. A key point is that probability is not a perfect tool for representing/describing uncertainties. One may, for example, assess that two different situations have probabilities equal to 0.2, but in one case the assignment is supported by a substantial amount of relevant data, whereas in the other by effectively no data at all. The likelihood judgement in itself does not reveal this discrepancy. When linking risk as a concept to a specific measuring device (likelihood, probability), special attention and care are warranted. The strength of the knowledge supporting the probabilities needs also to be highlighted, as well as the potential for surprises relative to this knowledge.

The IPCC reports also discuss knowledge strength, using the confidence concept summarizing judgements concerning evidence and agreement among experts. However, according to IPCC there is no link between the likelihood/probability judgements and the strength of knowledge judgements. Chapter 4 will show that there is in fact such a link and it is essential for understanding risk.

The recent IPCC reports also refer to risk as the "potential for consequences where something of value is at stake and where the outcome is uncertain, recognizing the diversity of values" (IPCC 2014a, p. 127). However, this broad understanding of risk is not followed up when it comes to the risk characterizations. Focus is on probabilities and expected values.

1.2 HOW TO DETERMINE THE BIGGEST GLOBAL RISKS?

How should we determine what are the most pressing global risks we face today? In its *Global Risk Reports* (WEF 2018), the World Economic Forum (WEF) provides an answer by presenting risk maps characterizing risk by impact and likelihood, using as input the result of a survey of experts and managers all over the world. If A symbolizes an event, like a natural disaster, water crisis or terrorist attack, the WEF approach presents values for the likelihood of A and its related impact. These values are averaged figures, based on the assignments made by the respondents. Five categories are used for both likelihood and impact. For the likelihood judgements, intervals are used (<20%, 21–40%, 41–60%, 61–80% and >80%), with reference to the event occurring in the next ten years. For the impact, only relative scores are used (minimal, minor, moderate, severe and catastrophic, with scores from 1 to 5, respectively).

This approach for characterizing risk raises several issues. First, the use of one impact value means that the respondents are forced to use a typical value or an expected value (the centre of gravity of their probability distribution for the impact, given the event occurring). This means that an important aspect of risk is not revealed: namely, that some events could have a much higher potential for extreme consequences than others. Secondly, the respondents will struggle with the probability assignments. It is a problem that the events considered are vaguely defined, with unclear links to the impact dimension. For example, a 'terrorist attack' could have a spectrum of consequences, some more severe than others, and, if one has in mind a 'typical impact level', the likelihood judgement would be completely different from that of the case where an extreme impact level was the reference point. In addition, there is no guidance provided on how to interpret the

likelihood judgements, which could also add an element of arbitrariness to the assessment process. It is also reasonable to question the use of averages in the analysis. Would it not be informative to reveal other aspects of the score distribution than the mean? A high spread may say something about the knowledge supporting these judgements.

This leads us to the third main challenge of the WEF approach to characterizing global risk. The strength of the knowledge supporting the judgements is not presented. Two events could have the same position in the risk matrix but be completely different with respect to the strength of the knowledge supporting the judgements. In one case, strong phenomenological understanding and data could be available; in other cases, we could face complete ignorance. The placing in the risk matrix could, however, be the same.

The WEF approach represents one way of characterizing global risk. Table 1.1 presents an overview of a set of existing theoretical perspectives for understanding risk, as well as methods for deriving the relevant knowledge supporting these perspectives, with the WEF approach placed. A distinction is made between three main categories of risk perspectives: risk viewed as expected consequences E[C], risk viewed as the pair: consequences and associated probability (C,P), and risk viewed as the pair: consequences and associated uncertainties (C,U). These will be explained and discussed in section 4.2. For the knowledge generation method, there is also a distinction between three categories. The first is based on hard data alone, the second on the use of expert judgements and the third on risk assessment, based on the modelling of phenomena and processes (as well as hard data and expert judgements). These methods for measuring or describing risk are discussed in more detail in section 4.2. The WEF approach is based on a mixture of the E[C] and (C,P) perspective and the use of expert judgements.

The WEF is the predominant study on global risk characterization. The approach used can also be applied on a national level; it is, however, more common to use risk assessment methods for this purpose; see for example

TABLE 1.1 Overview of how risk assessment studies depend on knowledge generation method and risk perspective

Knowledge generation method / Theoretical risk perspective	Hard data	Expert judgements	Risk assessments
Expected consequences (impact) E[C]		WEF 2018	OECD 2018
Consequences and probability (C,P)		WEF 2018	OECD 2018
Consequences and uncertainties (C,U)			OECD 2018

OECD (2009), Pruyt and Wijnmalen (2010), Veland et al. (2013), Vlek (2013) and Mennen and van Tuyll (2015). OECD (2018) provides a summary of national risk assessments (NRAs) for 20 countries and represents an excellent basis for studying current practice of the methods used. The OECD report highlights that the NRAs are used to inform public policy and identify challenges that the countries need to address to reduce risks. These references demonstrate that, for national risk assessments, in practice, we find all three types of underlying risk perspectives, E[C], (C,P) and (C,U), as illustrated in Table 1.1.

In Chapters 4 and 5, we will look more closely into these approaches for characterizing global and national risks, with suggestions for improvements. To evaluate the quality of the approaches, two main aspects are highlighted: validity and uncertainties. Validity relates to the degree to which one actually measures or characterizes what one sets out to measure or characterize, here global or national risks. Uncertainties relate to potential deviations between unknown quantities and the related estimated, predicted or assigned associated quantities, for example the deviation between the actual damage costs and their prediction, or between an underlying presumed true frequentist probability and its estimate. Hence, uncertainty is an aspect of validity.

The above discussion has focused on global and national risk. However, the coming analysis is, to a large extent, general and also applicable to other settings where the aim is to characterize risk.

1.3 QUANTITATIVE RISK ASSESSMENT AS A TOOL FOR ACCURATELY ESTIMATING RISK

For more than 40 years, Quantitative Risk Assessment (QRA) – also referred to as Probabilistic Risk Assessment (PRA) – has been used as the basis for supporting risk-related decisions in industry, in particular in the nuclear and oil/gas industries; see reviews by Rechard (1999, 2000). Its first application to large technological systems (specifically, nuclear power plants) dates back to the early 1970s (NRC 1975), but the key analysis principles have not changed much.

The basic analysis principles used can be summarized as follows (Aven and Zio 2011): a QRA systemizes the knowledge and uncertainties about the phenomena studied by addressing three fundamental questions (Kaplan and Garrick 1981):

- What can happen? (i.e. What can go wrong?)
- If it does happen, what are the consequences?
- How likely is it that these events and scenarios will occur?

Following this line of thinking, risk is calculated by computing probabilities for the events, scenarios and related outcomes, and expressed through metrics like the probability that a specific person shall be killed due to an accident (individual risk), the expected number of fatalities in terms of indices, such as PLL (Potential Loss of Lives) and FAR (Fatal Accident Rate), and f-n curves expressing the expected number of accidents (frequency f) with at least n fatalities.

Some improved methods have been developed in recent years to allow for increased levels of detail and precision in the modelling of phenomena and processes, for example to better reflect human and organizational factors, as well as software dynamics; see, for example, Mohaghegh et al. (2009) and Zio (2009, 2018).

The QRAs have, to a large extent, been built on a scientific framing, which is in line with natural sciences and the so-called scientific method (refer to section 2.2). The basic idea is that the system or activity studied possesses an inherent risk, which the assessment seeks to estimate as accurately as possible, using models, observational data and expert judgements. For more sophisticated QRAs, specific uncertainty analyses are used to express the uncertainties about the 'true' values of the risk (Paté-Cornell 1996).

Although it is acknowledged that the risk assessment is a tool to inform decision-makers about risk (Apostolakis 2004), common use of the assessments has, to a large degree, been rather 'mechanistic' (refer to discussion in Aven and Vinnem 2007). For example, it is common to see decision rules based on the results of the risk estimations: if the calculated risk is above a pre-defined probabilistic limit, risk is judged unacceptable (or intolerable) and risk-reducing measures are required, whereas if the calculated risk is below the limit, it is concluded that no measure is required or, alternatively, that measures should be subject to a broader cost-benefit type of consideration, in line with the so-called ALARP principle (As Low As Reasonably Practicable) (Aven and Vinnem 2007).

O'Brien (2000) gives a number of examples illustrating the implications for risk management of this use of risk assessments, most related to toxic chemicals. Although rather extreme and some would argue somewhat biased, her message is clear: risk assessments generally serve the interests of business (i), as well as government agencies (ii) and many analysts (iii) (Aven 2011c):

i) Through risk assessments an industry gets significant legal protection for activities that may result in contaminating communities, workers, wildlife, and the environment with toxic chemicals. Through risk assessment, industry gets protection for filling streams with sediments, thinning the ozone layer, causing high cancer rates, avoiding cleaning up its own messes, and earth-damaging activities (O'Brien 2000, p. 102).

The use of risk assessments gives the industry a scientific aura. The risk assessments show that the activities are safe, and most of us would agree that it is rational to base our decision-making on science. However, the complexity of a risk assessment makes it difficult to understand its premises and assumptions if you are not an expert in the field. In a risk assessment, there is plenty of room for adjustments of the assumptions and methods to meet the risk acceptance criteria.

In the case of large uncertainties in the phenomena and processes studied, the industry may be tempted to take advantage of the fact that in our society safety and environment-affecting activities and substances are considered innocent until 'proven guilty'. It takes several years to test, for example, whether a certain chemical causes cancer, and the uncertainties and choice of appropriate risk assessment premises and assumptions allow interminable haggling.

ii) Risk assessment processes allow governments to hide behind 'rationality' and 'objectivity', as they permit and allow hazardous activities that may harm people and the environment (O'Brien 2000, p. 106). The focus of the agencies is then more on whether a risk assessment has been carried out according to the rules than on whether it provides meaningful decision support.

iii) Risk analysts know that the assessments are often based on selective information, arbitrary assumptions and enormous uncertainties. Nonetheless, they accept that the assessments are used to conclude on risk acceptability.

This criticism of risk assessment is supported by a great deal of other research; see, for example, Reid (1992), Stirling (1998, 2007), Renn (1998b), Tickner and Kriebel (2006), Michaels (2008), Rae et al. (2014), Goerlandt et al. (2017) and Pasman et al (2017). Reid (1992) argues that the claims of objectivity in risk assessments are simplistic and unrealistic. Risk estimates are subjective, and there is a common tendency to underestimate the uncertainties. The disguised subjectivity of risk assessments is potentially dangerous and open to abuse if it is not recognized. According to Stirling (2007), using risk assessment, when strong knowledge about the probabilities and outcomes does not exist, is irrational, unscientific and potentially misleading. Renn (1998b) summarizes the criticism drawn from the social sciences over many years and concludes that technical risk analyses represent a narrow framework that should not be the single criterion for risk identification, evaluation and management. Tickner and Kriebel (2006, pp. 53–5) and Michaels (2008) argue along the same lines as O'Brien (2000). Tickner and Kriebel (2006) particularly stress the tendency of decision-makers and agencies not to talk about uncertainties underlying the risk numbers. Acknowledging

uncertainty can weaken the authority of the decision-maker and agency, by creating an image of being unknowledgeable. Precise numbers are used as a facade to cover up what are often political decisions. Michaels (2008) argues that mercenary scientists, including risk analysts, have increasingly shaped and skewed the technical literature, manufactured and magnified scientific uncertainty, and influenced government policy to the advantage of polluters and the manufacturers of dangerous products.

A main challenge of QRA relates to the use of causal chains and event analysis. This approach has strong limitations in analysing complex systems, as it treats the system as being composed of components with linear interactions, using methods like fault trees and event trees. These problems are addressed in resilience engineering and management, which argues for more appropriate models and methods for such systems (see e.g. Hollnagel et al. 2006). Alternative methods have been developed, of which FRAM and STAMP are among the most well-known (Hollnagel 2004, Leveson 2004, 2011).

Nonetheless, risk assessments and QRAs based on linear models are still commonly used and guide decision-makers. They seem to provide some value. In this book, we will look further into the scientific basis of risk assessments and QRAs. The topic was discussed as early as in 1981 by Cumming and Weinberg in the editorials of the first issue of the journal *Risk Analysis* (Cumming 1981, Weinberg 1981) in relation to the establishment of the Society for Risk Analysis (SRA). Both editorials conclude that risk assessment comprises scientific elements but is not a scientific method *per se*, as accurate risk estimation and predictions cannot be obtained in the case of large uncertainties. Nearly 40 years later, we may ask: is this conclusion still valid? And if it is, how can it then be that QRAs are commonly used in this way, to accurately estimate risk and claim to know the truth about risk? Is it possible to formulate conditions for when this approach is scientific and when it is not?

Fortunately, alternatives to this way of framing and using risk assessments exist. Risk assessment can also be seen as a tool for representing or expressing the knowledge and lack of knowledge available. What does this change really mean – in relation to assessments but also with respect to use of the assessments? Is risk assessment then more scientific and how? This we will discuss in coming chapters, section 2.2 and Chapter 5 in particular.

1.4 SECURITY RISKS: THE ALLEGATION THAT SMALL RISKS ARE TREATED OUT OF PROPORTION TO THEIR IMPORTANCE

The point of departure for this case is the book, *Thinking Fast and Slow*, by Daniel Kahneman (Kahneman 2011). The book is based on a dichotomy

between two modes of thought: *System 1*, which operates automatically and quickly, instinctively and emotionally, and *System 2*, which is slower, more logical and deliberative. The book identifies cognitive biases associated with each type of thinking, using several decades of academic research on the issue, to a large extent linked to Kahneman's own research; see section 6.1.

The book also relates to risk. Kahneman asserts that we have a basic lack of ability to treat small risks: we either ignore them completely or give them too much weight. The main thesis put forward is that we overestimate small risks (Kahneman 2011, p. 324).

The present book questions these views. A security case is here used to illustrate the discussion, but the insights are general and also applicable to problems related to technology and engineering, environmental impacts and natural disasters, health or financial risk management. All areas are concerned with managing small risks.

The example to be discussed is related to suicide bombings on buses in Israel in the period 2001–4:

> I visited Israel several times during a period in which suicide bombings in buses were relatively common – though of course quite rare in absolute terms. There were 23 bombings between December 2001 and September 2004, which had caused a total of 236 fatalities. The number of daily bus riders in Israel was approximately 1.3 million at that time. For any travel, the risks were tiny, but that was not how the public felt about it. People avoided buses as much as they could, and many travellers spent their time on the bus anxiously scanning their neighbours for packages or bulky clothes that might hide a bomb.
>
> I did not have much occasion to travel on buses, as I was driving a rented car, but I was chagrined to discover that my behaviour was also affected. I found that I did not like to stop next to a bus at a red light and I drove away more quickly than usual when the light changed. I was ashamed of myself, because of course I knew better. I knew that the risk was truly negligible, and that any effect at all on my actions would assign an inordinately high 'decision weight' to a minuscule probability. In fact, I was more likely to be injured in a driving accident than by stopping near a bus. But my avoidance of buses was not motivated by a rational concern for survival. What drove me was the experience of the moment: being next to a bus made me think of bombs, and these thoughts were unpleasant. I was avoiding buses because I wanted to think of something else.
>
> (Kahneman 2011, pp. 322–3)

The problem with this analysis is that the individual risk is not determined by hindsight, observing historical fatality rates. At a specific point in time,

an objective risk metric for this person does not exist. The statement that the individual risk is minimal lacks a rationale, as risk relates to the future and the future is not known. Thus, the associated behaviour cannot be said to be irrational (in a wide sense of the word), as there is no way to determine the truth about risk at the decision point. We can make the same considerations concerning probability. Kahneman seems to link probability to historical observations, not to the future and to judgements about the future. He refers frequently to the "exact probability level" – for example, he writes on p. 323: "The emotion is not only disproportionate to the probability, it is also insensitive to the exact level of probability." However, there is no objective probability that can be used as a basis for a proper decision weight. The thinking fails to take into account the uncertainty dimension. Risk and probability are referred to as being objective quantities for which rational comparisons can be made. Such concepts do not exist in the example addressed here or in most other real-life situations. Note that the criticism here relates to what Kahneman writes about risk and probability in this particular case, not to his work in general, which is indeed impressive and strong.

Kahneman continues with another example, linked to lotto. He points to a similarity: buying a lotto ticket gives an immediate reward of pleasant fantasies, as avoiding the bus is immediately rewarded by relief of fear. According to Kahneman, the actual probability is inconsequential for both cases; it is only the possibility that matters (Kahneman 2011, p. 323). However, the two situations are not comparable; in the latter case, there is an objective probability that we can relate to, but not in the former case. It is this lack of objective reference values that makes risk so difficult to measure and handle. Kahneman and his school of thought have for decades conducted research that shows that people (and in particular laypersons) are poor assessors of probability, if the reference is an objective, true probability, and that probability assignments are influenced by a number of factors (Tversky and Kahneman 1974). It has been shown that people use rather primitive cognitive techniques when assessing probabilities; these are *heuristics*, which are easy and intuitive ways to specify probabilities in uncertain situations. The result of using such heuristics is often that the assessor unconsciously tends to put too much weight on insignificant factors. The most common heuristics are the availability heuristic, the anchoring and adjusting heuristics and the representativeness heuristic; see also section 6.1.

But, if it is not possible to relate the probability assignment to a true value, how can we then speak about biases and poor assessments? For an individual taking the bus in the above example, the research framework of Kahneman and others may be questioned, as the event is a unique event for this person. Of course, he or she may benefit from the general insights provided by the research of biases and heuristics, for example the availability

heuristic, which means that the assessor tends to base his probability assignment on the ease with which similar events can be retrieved from memory; events where the assessor can easily retrieve similar events from memory are likely to be given higher probabilities of occurrence than events that are less vivid and/or completely unknown to the expert. There exists, however, no reference for making a judgement that this heuristic leads to a bias. Care must be shown when applying the results from the research framework of Kahneman and others to unique events. It can lead to unjustified conclusions, as in the above example, where the 'true' probability of being killed in a bus bombing was said to be negligible.

Kahneman is not alone in thinking along these lines. The literature is filled with contributions in which the same type of reasoning prevails. Authors lampoon the way society deals with security issues – the terrorist risks are overestimated; very small risks are treated out of proportion to their importance.

For example, the message from Omdal (2009) and Hammerlin (2009) is that the terrorist risk is fictional. It is argued that there is a greater risk of drowning than being hit by a terror attack. They point to research showing that there is no scientific basis for claiming that the security controls at airports make it safer to fly, and that the statistical probability of dying in a terrorist attack in the West is 0.0000063; since 11 September 2001, more people have drowned in the bathroom in the US than have been killed in terrorist attacks. Terror is not something to fear, says Hammerlin, as the risk is microscopic. The population is frightened by a fictitious danger and risk. Is it any wonder that the authors are upset and lampoon the authorities?

Do these authors completely ignore that the current security measures are working and that the figures would have been different without these measures? Again, the reference seems to be some underlying true risk, which is provided by the observed historical numbers. The authors take a blinkered view of what has happened. But there is a big leap from history to the future. And it is the future that we are concerned about. What will happen tomorrow, what form will an attack take and what will the consequences be? We do not know. There is uncertainty associated with these events and their consequences.

Numbers expressing the risk can be given, but they will always be dependent on the available knowledge and the assumptions made. The historical data referred to by Hammerlin say something about the risk, but the most important aspect of risk is not addressed, namely, uncertainty; we do not know what is next. We hope that the security measures implemented can prevent a terrorist attack, but they are also motivated by a need to reduce uncertainty and make people feel more secure. However, if the underlying perspective is that the risk is objectively described by a risk number, such arguments will be of little interest.

1.5 THE CALL FOR A SHIFT FROM RISK TO RESILIENCE

In recent years, calls have been made for a shift from risk to resilience, for example by the former UN Secretary-General Ban Ki-moon (UNISDR 2015). The basic idea is that we need to be prepared when threatening events occur, whether they are anticipated or unforeseen. Is the call based on a belief that the risk field and science should be replaced by resilience analysis and management, or is it more about priorities: more weight should be placed on improving resilience?

Over the last decades, a new field has developed – resilience analysis and management (see e.g. Holling 1973, Flach 1988, Rutter 1993, Leveson 2004, Hollnagel et al. 2006, Hollnagel 2010, Renn 2008, Haimes 2009, Bhamra et al. 2011, Francis and Bekera 2014, Linkov et al. 2014, Righi et al. 2015, Woods 2015 and Le Coze 2016). The field is rapidly developing, and we see today applications in many different areas. Resilience thinking is, for example, increasingly influencing policy documents related to disaster and crisis management.

But what is the relationship between this field and risk analysis, as interpreted in this book? The resilience field arose as a supplement to the traditional probabilistic risk assessment approach, which has strong limitations in analysing many types of real-life systems, in particular complex systems, which are characterized by large uncertainties and a potential for surprises. By strengthening the resilience of the system, the safety is enhanced without a need to perform risk calculations. For example, by strengthening the immune system, the resilience is improved, and the person is less likely to become sick when exposed to, for example, infectious organisms. The attractiveness of the resilience approach is that we do not need to know what type of events – hazards and threats – can occur and to express their probabilities as needed in traditional risk assessments.

Nonetheless, there is a link between resilience and risk. Improved resilience reduces the risk of undesirable consequences of the activity studied. The relationship is, however, not straightforward, as discussed, for example, by Haimes (2009), Aven (2017d), Park et al. (2013) and Linkov et al. (2016). Two 'schools' seem to develop: one highlighting risk, the other resilience. Although works have been conducted to integrate the two perspectives (Haimes 2009, Aven 2017d, Park et al. 2013, Linkov et al. 2016), we also see tendencies for separation. It is, for example, conspicuous that a lot of research on resilience completely ignores considerations of risk, and vice versa.

As mentioned above, a call for a shift from risk to resilience has recently been put forward. At the first glance, the call seems to indicate that risk analysis should be replaced by resilience analysis and management. Alternatively,

it may indicate a change in focus and weight. However, for both interpretations, the call could have serious implications for risk analysis as a field and science. It relates to its place as an academic discipline, the availability of and interests in study programmes at universities and colleges, the potential for research funding, and its influence as a field and science in society in general. It is therefore important to look more closely into the rationale for the call.

The call will be addressed in coming chapters, particularly section 7.4. The discussion aims at enhancing our understanding of these two fields and their interrelationships. More specifically, we question to what extent the basic resilience thinking conflicts with the knowledge and guidance provided by today's risk analysis field and science. Is it so that the resilience field challenges the current ideas, principles and methods of risk analysis? Is the resilience field to be considered a distinctive field and science in parallel to risk analysis, or should risk analysis be considered the overriding concept and field, and resilience a supporting pillar for this field? If we study current risk management and governance frameworks, resilience is a key strategy for handling risk (Renn 2008). Does the call argue that the resilience strategy should be highlighted at the expense of the broader frameworks for handling risk?

1.6 THE DEVELOPMENT OF A RISK GOVERNANCE FRAMEWORK

This section reviews basic risk governance literature and theory, related to the concept of systemic risk, as well as the terms, 'complex', 'uncertain' and 'ambiguous risk problems'. The section provides a background for the discussion in coming chapters, particularly section 3.2, which addresses different types of research and research methods used in risk analysis, and section 7.6, which looks more closely into some of the conceptual challenges that the risk governance area faces. The example aims at illustrating how risk research develops.

1.6.1 The risk governance concept

The concept of 'risk governance' was introduced to the academic discourse through European networks on risk at the turn of the millennium (Hood et al. 2001, IRGC 2005, Renn 2008, van Asselt and Renn 2011). The concept was introduced to meet a need for proper risk handling – where we have many actors, individuals and institutions, public and private – for specific challenging risks or risk problems. Using governance principles, a new approach to the identification, assessment, management and communication

of risk has been developed. What characterizes these risks and risk problems is a key to understanding the scope of risk governance. Several model structures for such characterizations have been developed (Funtowicz and Ravetz 1985, 1994, Hood et al. 2001, IRGC 2005, Renn 2008, van Asselt and Renn 2011, Pritchard 2015, Harvey 2018). Here, we address two of these, which have both received considerable attention in the literature. The first states that these risk problems are those characterized as complex, uncertain and ambiguous, in contrast to simple risk problems, where probabilistic analyses provide a suitable structure, such as for car accidents and smoking (IRGC 2005, Renn 2008). The second relates these risk problems to the notion of "systemic risk" (OECD 2003, Renn 2016), which, according to Renn (2016), can be characterized by the following four features: they are (1) global in nature, (2) highly interconnected and intertwined, leading to complex causal structures, (3) nonlinear in their cause–effect relationships, and (4) stochastic in their effect structure; see section 1.6.3.

From the fundamental work on risk governance some 10–15 years ago, considerable efforts have been made to further strengthen the scientific basis of the risk governance concept. Van Asselt and Renn (2011), Aven and Renn (2010, 2015, 2019) and Renn (2016) provide examples of contributions to this end, with their conceptual analysis of key terms.

The SRA (2015a) Glossary defines 'risk governance' in this way (based, to a large extent, on IRGC (2005) and Renn (2008)):

> Risk governance is the application of governance principles to the identification, assessment, management and communication of risk. Governance refers to the actions, processes, traditions and institutions by which authority is exercised and decisions are taken and implemented. Risk governance includes the totality of actors, rules, conventions, processes, and mechanisms concerned with how relevant risk information is collected, analysed and communicated and management decisions are taken.
>
> (SRA 2015a)

The concept of risk governance resembles the fundamental building blocks of the concept of 'risk analysis', as defined by the Society for Risk Analysis since 1980, mainly in the USA, as defined in the Preface. Using 'risk analysis' in this way, we can interpret 'risk governance' as the application of governance principles throughout all the components of risk analysis. Following this understanding of risk governance, we need to look further into what 'governance principles' means. Comprehensive discussions can be found in, for example, van Asselt and Renn (2011), Renn (2008) and Aven and Renn (2010). As stated by van Asselt and Renn (2011), the concept of 'governance'

came into fashion in the 1980s. A basic idea was that government is not the only actor involved in managing and organizing society. This can be seen as a reaction to new challenges, including globalization, increased international cooperation, societal changes, such as the increased engagement of citizens and the rise of non-governmental organizations (NGOs), the increasing complexity of policy issues and the resulting difficulty in making decisions with confidence and legitimacy (van Asselt and Renn 2011, Pierre and Peters 2000, Walls et al. 2005). Governance is relevant for different 'zones', such as in the 'global space', in the 'national space', for organizations and for communities (Graham et al. 2003).

What constitutes good principles of governance is subject to discussion, but Openness, Participation, Accountability, Effectiveness, Coherence and Proportionality/Subsidiarity are commonly seen as key principles of good governance (EC 2001, Aven and Renn 2010). Graham et al. (2003) refer to five fundamental principles based on the United Nations Development Programme: Legitimacy and Voice (participation and consensus orientation), Direction (strategic vision), Performance (responsiveness and effectiveness/efficiency), Accountability (transparency) and Fairness (equity, rule of law). Similar formulations are, for example, stated by the Council of Europe (2017) through their 12 principles: Fair Conduct of Elections, Representation and Participation; Responsiveness; Efficiency and Effectiveness; Openness and Transparency; Rule of Law; Ethical Conduct; Competence and Capacity; Innovation and Openness to Change; Sustainability and Long-term Orientation; Sound Financial Management; Human Rights, Cultural Diversity and Social Cohesion; and Accountability. These are just examples; it is possible to find many other suggestions in the literature for what constitutes good governance. However, for the purpose of the present analysis, they are sufficient. We see the contours of a set of important principles, and there will obviously be a need for processing if we are to apply these principles to risk: what principles should be highlighted and what aspects should be prioritized when applying these principles to the risk handling?

Developing a risk governance field from such principles is not straightforward and requires considerable research. The 'International Risk Governance Council (IRGC) school of thought' has followed some ideas and directions, as illustrated by the work of van Asselt and Renn (2011), in which the authors suggest three principles of risk governance: Communication and Inclusion; Integration; and Reflection. Communication here refers to interactions in which knowledge, experiences, interpretations, concerns and perspectives are exchanged between policy-makers, experts, stakeholders and the general public, and among themselves. Inclusion can take different forms: roundtables, open forums, negotiated rule-making exercises, mediation or mixed advisory committees, including scientists and stakeholders.

Integration refers to the need to collect and synthesize all relevant knowledge and experience from various disciplines and various sources, including uncertainty information and articulations of risk perceptions and values. The third reflection principle highlights the need for a collective reflection balancing the pros and cons between development and protection.

1.6.2 Risk and risk-problem classification system

This section briefly summarizes the commonly used classification system to distinguish between different types of risks and risk problems, using the four categories: simplicity, complexity, uncertainty and ambiguity (IRGC 2005, Renn 2008, Aven and Renn 2010). Some minor adjustments have been made in the formulation, as defined in some of these references, to simplify the analysis and highlight key points.

First, let us clarify the terminology. Is smoking a risk or an activity? The answer depends of course on how we define risk. It is common in the literature to refer to smoking as a risk, but, in this book, we follow the established nomenclature developed by the Society for Risk Analysis (SRA) and refer to smoking as an activity which is associated with risk (SRA 2015a). Smoking can be viewed as a risk source. A similar interpretation is made for an event like flooding. It is commonly referred to as a risk but, in this book, is referred to as a hazard or a threat. See Chapter 4.

The label 'simple risk' – for smoking, for example – will consequently not be used. What are 'simple' are the risk's features, its characterization, perception and/or handling. We talk about the features of the risk issue or problem considered. To simplify the nomenclature, we refer to the risk problem being simple.

A risk problem is simple if it is possible to quite accurately predict the occurrence of events and/or their consequences. The connection between a triggering event or activity such as smoking and the negative consequence such as lung cancer is fairly straightforward and can be captured by a reliable probability distribution over potential outcomes of smoking. The risk problem is not characterized by complexity, uncertainty and/or ambiguity as defined below.

A risk problem is complex if it is difficult to accurately predict the performance of the system (activity) considered, based on knowing the specific functions and states of the system's individual components (based on knowing the individual performance of the sub-activities of the activity). Critical infrastructures like electric grids, telecommunication networks, railways, healthcare systems and financial circuits are examples of complex systems. In these cases, there are many intervening variables between a trigger and its effect, thus amplifying, attenuating or even impeding the original causal or functional relationship.

A risk problem is uncertain if it is difficult to accurately predict the occurrence of events and/or their consequences. The uncertainty can be due to, for example, incomplete or invalid databases, variation, lack of phenomenological understanding and modelling inaccuracies. An example of an uncertain risk problem is 'terrorism risk'. Here, although the consequences of an attack can be fairly accurately predicted, the type and time of attack is subject to considerable uncertainties. Hence, any probability distribution established on the basis of historical data and related statistical analysis will be a weak predictor for the future. Context conditions may change, and human agency is involved as a modifier between causes and effects.

A risk problem is ambiguous if there are different views on:

> [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)
>
> (Aven and Renn 2010, p. 13)

A classic example to illustrate interpretative ambiguity is neuronal activities in the human brain; what does it mean that these activities are intensified when subjects are exposed to electromagnetic radiation (Aven and Renn 2010, p. 13)? Is the change to be interpreted as an adverse effect or is it simply a bodily response without any implication for health?

Examples of problems with normative ambiguity are passive smoking and nuclear energy. Should we allow smoking, if individuals are aware of the health implications of smoking? Should we use nuclear energy, even if the majority of people in a given country are opposed to it?

Simplified, interpretative ambiguity is understood as ambiguity of evidence but not of values, and normative ambiguity is ambiguity of values but not of evidence (Renn 2008, p. 151). From these different categories of risk problems, a set of risk management strategies, using various instruments, is recommended (IRGC 2005, Renn 2008, Aven and Renn 2010).

Many other ways of characterizing risks and risk problems have been suggested in the literature. For risk-governance settings, the above one from IRGC is by far the most commonly referred to.

1.6.3 Systemic risks

The concept of "systemic risk" was introduced by OECD (2003, p. 9) to address risks that affect the systems on which society depends, like health, transport, environment, telecommunications, etc. Since then, considerable work has been conducted to further develop the concept; see, for example, van Asselt and Renn (2011) and Renn (2016). According to Renn (2016),

a widely cited definition of a systemic risk is provided by Kaufman and Scott (2003): "Systemic risk refers to the risk or probability of breakdowns in an entire system, as opposed to breakdowns in individual parts or components, and is evidenced by co-movements (correlation) among most or all parts". Following up this definition, Renn (2016) states that it is the totality of the threat, the probability that the entire system can collapse, that distinguishes systemic from other types of risk. According to van Asselt and Renn (2011), systemic risks are complex and surrounded by uncertainty and/or ambiguity.

Work on systemic risk – such as for problems that are complex, uncertain and/or ambiguous – acknowledges that conventional approaches for risk assessment and management are not sufficient. Broader frameworks are required, such as the IRGC framework (IRGC 2005, Renn 2008, Aven and Renn 2010). Three types of risk-management strategies form the basic building blocks of these frameworks: risk-informed (using risk assessments), cautionary/precautionary and discursive strategies (Renn 2008, SRA 2015b); see Chapter 7. The cautionary/precautionary strategy can also be seen as a strategy of robustness and resilience. In practice, the appropriate strategy will be a mixture of these three types of strategies. The ideas of the so-called analytic-deliberative processes (Stern and Fineberg 1996) also constitute key pillars of these types of frameworks (Renn 2016).

1.6.4 Research process

The research conducted to develop the risk governance concept – the framework – is a combination of conceptual and empirical work, as explained and discussed in section 3.2.1. Conceptual research will be given special attention in this book. Many, both academics and practitioners, are not so familiar with this category of research. This type of research relates to concepts, theories, principles, approaches and methods, and we will look more closely into what defines and characterizes this type of research. How does it relate to empirical research? And how is it evaluated?

2 Fundamentals about science, knowledge and research

This chapter provides a general introduction to science, knowledge and research, and forms a platform for the risk analysis science to be presented in the next chapter. First, we give a brief introduction to the term 'science', then a discussion of its relationship to knowledge.

2.1 SCIENCE

The English word 'science', with its counterparts in the Romance languages, covers a rather limited group of disciplines, compared to its translations into the other Germanic languages such as 'Wissenschaft' (German), 'wetenschap' (Dutch), 'vitenskap' (Norwegian) and 'vetenskap' (Swedish). Originally the word 'science' had a very broad meaning, covering nearly every type of knowledge or skill that is acquired through study, be it prosody or horse-riding. In the 1600s and 1700s, the meaning of the term was restricted to systematic knowledge, and during the 1800s it was further restricted to denote the new, more empirical type of knowledge in the area previously called 'natural philosophy'. The word 'science' is still often used as a synonym for 'natural science', but it is also applied to some of the academic areas in the behavioural and social areas. Economics and sociology are often counted as sciences, whereas other academic disciplines, such as those concerned with human history, arts and literature, are not. 'Wissenschaft' and its cognates in the other Germanic languages originate from words with a similar original meaning to that of 'science', namely as a general synonym for 'knowledge'. 'Wissenschaft' is now similar in meaning to 'science' but with the important difference that it covers all the academic fields, including the humanities.

Terminology can be important, but even more important is the existence of a community of knowledge disciplines, each of which searches in a systematic

way for valid knowledge in its own subject area. Due to their different subject areas, the knowledge disciplines differ widely in their methodologies – from interpretations of ancient texts to calculations based on recordings of particle collisions in a synchrotron. Nevertheless, they are united by a set of common values, including the tenet that truth claims should be judged according to universal and impersonal criteria, as independently as possible of the value-based convictions of the individual scientist. Importantly, the knowledge disciplines are also connected through an informal but nevertheless well worked-out division of intellectual labour. The disciplines that are part of this community respect each other's competences; this also applies across the supposed barrier between the 'sciences' (in the traditional, limited sense) and the humanities. An astronomer who wishes to understand ancient descriptions of celestial phenomena has to rely on philologists in issues of text interpretation, and, similarly, an archaeologist has to ask biologists for help to identify seeds found in an ancient jar.

Thus, the community of knowledge disciplines includes not only those usually called 'sciences' but also others that fall under the designation of Wissenschaft. In its entirety, the community covers a wide array of subject areas that can be summarized under five headings (Hansson 2013a):

- nature (natural science),
- ourselves (psychology and medicine),
- our societies (social sciences)
- our own physical constructions (technology, engineering)
- our own mental constructions (linguistics, mathematics, philosophy).

Many attempts have been made to specify the type of knowledge that is characteristic of science by means of specifying or delimiting the methods or methodologies that give rise to scientific knowledge. Probably the best known among these is Karl Popper's falsifiability criterion, according to which "Statements or systems of statements, in order to be ranked as scientific, must be capable of conflicting with possible, or conceivable observations" (Popper 1962, p. 39). This and other such proposals are intended to be directly applicable to concrete issues of demarcation. For any given activity, such a criterion should be able to tell us whether or not it is scientific. However, all such criteria have severe problems. Most of them are suitable only for some, not all, of the disciplines of science, and all of them tend to exclude the science of previous centuries as unscientific, although it was the best of its day.

The failure of such method-based definitions of science should be no surprise. What unites the sciences, across disciplines and over time, is the basic commitment to finding the most reliable knowledge in various

disciplinary areas. The term 'reliability' is used in the standard epistemological sense of being obtained in a truth-conducive way (Hudson 1994).

The precise means to achieve this knowledge generation differ among subject areas, and the chosen methods are also in constant development. The major strength of science is its capability of self-improvement. Many of its most important self-improvements have been methodological, and these improvements have repeatedly been so thorough as to change not only the detailed methods but also high-level general methodological approaches, including principles for hypothesis testing, the acceptability of different types of explanations, and general experimental procedures such as randomization and blinding. Therefore, a methods-based delimitation of science can only have temporary validity (Hansson 2013a).

We seek a definition of science which is fully general and therefore not time-bound. Consequently, such a definition cannot by itself determine in each particular case what is and is not science. Following Hansson (2013a), we are led to this definition:

> Science (in the broad sense) is the practice that provides us with the most reliable (i.e. epistemically most warranted) statements that can be made, at the time being, on subject matter covered by the community of knowledge disciplines, i.e. on nature, ourselves as human beings, our societies, our physical constructions, and our thought constructions.
>
> (Hansson 2013a)

From this, a specific science can be delineated by restricting it to its relevant knowledge discipline.

Often the criteria, explanatory power and usefulness, are added to the requirement of the 'epistemically most warranted statements' (Hansson and Aven 2014). In practice, aspects of usefulness are always an issue when discussing knowledge production. A new concept can be suggested, and strong arguments provided, but if it has no applicability it could soon be ignored. However, history has shown that care must be taken when making judgements about usefulness, as what was previously seen as of purely theoretical interest suddenly becomes a hot topic, with a huge potential for applications.

The explanatory power criterion is also problematic. Consider the statistical science. It can be defined as the science of collecting, analysing, presenting, and interpreting data (Gregersen 2011). Does it have explanatory power? Is the science producing methods that allow us to produce accurate predictions? Yes, in statistics – often together with other disciplines like medicine, engineering and natural sciences – considerable efforts are made to develop methods to obtain such predictions. Yet, the science of statistics as such does not depend on success in this respect for any situation.

Statistics has limited explanatory power in many cases, in particular when the data are few or not relevant. However, the field and science of statistics still deliver knowledge about how to make predictions and understand and treat uncertainties. This knowledge has strong limitations in the sense that only some types of uncertainties are dealt with, at least when considering the traditional statistical science. Nonetheless, there is no discussion about whether statistics is a science or not.

In line with these ideas and categorization, in this book, we will use the term 'science' in a broad sense that captures the disciplines denoted in German as 'Wissenschaften'. Risk analysis is considered in this community of knowledge disciplines, not only among the disciplines conventionally covered by the English word 'science'.

A distinction is made between a specific science as a field or discipline, and the knowledge generation of the science. The discipline covers the totality of relevant educational programmes, journals, papers, researchers, research groups and societies, etc. The latter part covers the knowledge produced by the discipline, for example in medicine, knowledge about diseases and how to best treat these (see Figure 2.1).

2.1.1 Norms and values in science

Scientific practice is characterized by a set of norms and values that is remarkably similar across the disciplines. Historians, mathematicians and biologists alike expect their colleagues to be open to criticism, disclose information that speaks against their own hypotheses, and attempt to get every detail right. An influential attempt to summarize these standards was made

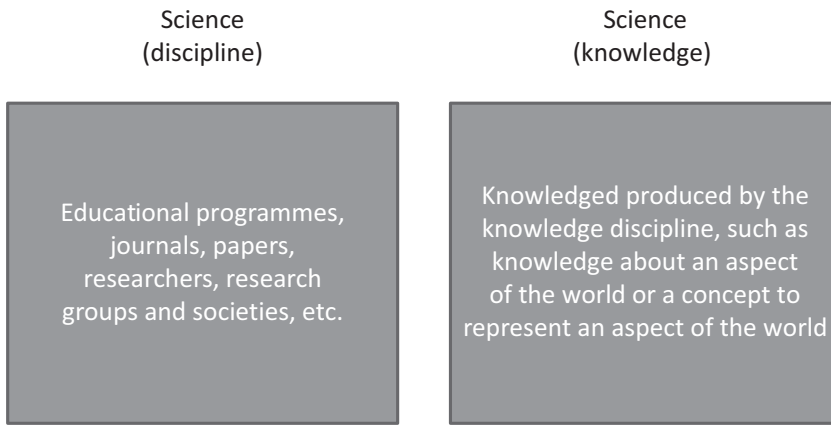


FIGURE 2.1 An illustration of the difference between a science as a discipline (field) and the knowledge part of the science

by the sociologist Robert K. Merton ([1942] 1973). According to Merton, science is characterized by an ethos or spirit that can be summarized as four sets of institutional imperatives.

The first of these, *universalism*, asserts that, whatever their origins, truth claims should be subjected to pre-established, impersonal criteria. This implies that the acceptance or rejection of claims should not depend on the personal or social qualities of their protagonists.

The second imperative, *communality*, says that the substantive findings of science are the products of social collaboration and therefore belong to the community, rather than being owned by individuals or groups. According to Merton, this is incompatible with patents that reserve exclusive rights of use to inventors and discoverers. (Merton originally used the rather infelicitous term 'communism'; for obvious reasons, 'communality' is preferable.)

His third imperative, *disinterestedness*, imposes a pattern of institutional control that is intended to curb the effects of personal or ideological motives that individual scientists may have. The fourth imperative, *organized skepticism*, implies that science allows detached scrutiny of beliefs that are dearly held by other institutions. This is what sometimes brings science into conflict with religions and other ideologies.

In popular discussions, science is often described as being ideally 'value-free'. That is impossible; values such as those associated with Merton's four imperatives are necessary as guidelines in scientific activities. But there is an important kernel of truth in the ideal of a value-free science. Although science neither can nor should be free of all values, there are many types of values that we require scientists to be as little influenced by as possible in their scientific work. In particular, we expect their factual statements to be as unaffected as possible by their religious, political or other social convictions.

There are two categories of values (and norms) that have a claim to be accepted in science and integrated in the scientific process. The first of these are what philosopher Carl Hempel termed the "epistemic" values. These are values that support the scientific process itself: the values of truth and error-avoidance, the values of simplicity and explanatory power in hypotheses and theories (Hempel 1960, Feleppa 1981). The presence of such values in science is generally recognized by philosophers of science.

The second category is much less often discussed or even recognized: non-controversial social and ethical values, i.e. values that are shared by virtually everyone or by everyone who takes part in a particular discourse. The presence of non-controversial values in science is often overlooked, since we tend not to distinguish between a value-free statement and one that is free of controversial values. Medical science provides good examples of this. When discussing analgesics, we take for granted that it is better if patients have less rather than more pain. There is no need to interrupt a medical discussion in

order to point out that a statement that one analgesic is better than another depends on this value assumption. Similarly, in economics, it is usually taken for granted that it is better if we all become richer. Obviously, a value that is uncontroversial in some circles may be controversial in others. This is one of the reasons why values believed to be uncontroversial should be made explicit and not treated as non-values. Nevertheless, the incorporation of uncontroversial values, such as the basic precepts of medical ethics, will have to be recognized as reasonable in applied science, provided that these values are not swept under the rug but instead openly discussed and taught and put to question whenever they become less uncontroversial than they were thought to be.

2.2 KNOWLEDGE

It is common to distinguish between three types of knowledge: know-how (skill), know-that of propositional knowledge and acquaintance knowledge. "Knowing how to go skiing" is an example of know-how, and the statement "I know that Norway is a country in Europe" is an example of propositional knowledge, while "I know Peter" is an instance of the acquaintance knowledge. Propositional knowledge, but also aspects of know-how, are the focus in this book.

In the literature, (propositional) knowledge is most commonly understood as "justified true beliefs" (SEP 2011). However, this way of thinking in relation to knowledge can be challenged, and this book considers knowledge to be justified beliefs. Think as an example about a person who is to estimate the frequentist probability of a specific die showing '1' in a trial. The person studies the die and argues that, because of symmetry, the probability is 1/6. Now, if knowledge is to be seen as 'justified true beliefs', we cannot conclude that the assessment represents knowledge, as the truth is not known. However, would it not be reasonable to say that the judgement represents some knowledge? Yes, it would, but then knowledge must be understood as 'justified beliefs' and not 'justified true beliefs'. As another and related example, think about a research team that is to estimate the fraction of people in a population who suffer from a specific disease. The team performs a risk assessment, which includes a statistical analysis of a sample of the population and makes some conclusions. Again, this assessment cannot be seen as knowledge, if 'justified true beliefs' is the definition, as the true fraction is not available. However, if 'justified beliefs' is the criterion, knowledge is gained. The examples show that the 'justified true beliefs' definition is not suitable for risk analysis. The true outcome of future events cannot be known with certainty; nevertheless, we can have knowledge about this future.

Following this line of thinking, knowledge is not objective, as a belief is someone's belief. In general, we have to look at knowledge as subjective or at best inter-subjective among people, for example, experts.

The 'justified beliefs' interpretation of knowledge is in line with, for example, recommendations by SRA (2015a), and we find a number of definitions of knowledge in the literature which support this way of understanding knowledge, although it is not common in the philosophical literature (see e.g. Aven and Ylonen 2018). The perspective taken is also in line with the understanding of science adopted in this book and described in Section 2.1. Science is considered to be the most warranted statements – or, rephrased, the most justified beliefs – generated by the relevant knowledge discipline. Hence, we can distinguish between knowledge as justified beliefs and science as the most justified beliefs of the knowledge discipline.

The knowledge field of statistics may, for example, have concluded that frequentist probability is the most warranted (justified) representation of variation in populations. However, deciding what are the most warranted statements (justified beliefs) is often an issue, for example, on how to best represent uncertainties in risk analysis. There is a continuous battle on what these statements are – it is about institutions and power. Different directions and schools of thought argue for their beliefs, trying to obtain control over the field (Bourdieu and Wacquant 1992).

The knowledge and science perspective adopted here means that the knowledge can be more or less strong and also erroneous. The statements and beliefs can be more or less justified or warranted. The perspective avoids taking a stand on philosophical issues related to positivism, relativism and related philosophical doctrines, which have been thoroughly discussed in the literature (see e.g. Walliman 2011). An 'objective truth' may be considered to exist in some cases but not in others.

2.3 RESEARCH (KNOWLEDGE GENERATION)

Research is the production of knowledge and represents a key element of a science discipline; see Figure 2.1. The knowledge can be generated in different ways. It is common to distinguish between two main approaches:

The first one relates to empiricism, which seeks to gain knowledge about an aspect of the world by gathering observations through systematic scientific methods. The second approach is rationalism, which refers to the understanding that, through reasoning, we can know. The starting point is some general statements (premises) and, through logical argument, a specific conclusion is derived (Walliman 2011).

In practice, combinations of these two approaches are used. Most known is the 'hypothetico-deductive method', also referred to as the 'scientific method'. It can be seen as comprising the following four steps (Wolfs 2009):

1. Observations and descriptions of a phenomenon
2. Formulation of a hypothesis to explain the phenomenon, for example using a mathematical relationship
3. Use of the hypothesis to predict the existence of other phenomena or to predict the results of new observations
4. Performance of experimental tests to verify or falsify the hypothesis.

Statistical inference provides the common framework for carrying out this method.

The hypotheses form the theories (models) on which the research is based. As stated by Deming (2000, pp. 102–3), "Rational prediction requires theory and builds knowledge through systematic revision and extension of theory based on comparison of prediction with observation." "Without theory, experience has no meaning", . . . and "Without theory there is no learning."

Generating knowledge is also about other types of processes, in particular social processes. Knowledge is subject to a constant construction process, strongly affected by power aspects, as mentioned in Section 2.2, as well as specific historical, economic and social conditions (e.g. Lincoln and Guba 2000, p. 177, Bourdieu and Wacquant 1992, Scheler 1980, Mannheim 1979); see also Aven and Ylonen (2018).

Expert consensus may be considered a criterion in relation to this social constructionist approach. However, consensus can be the result of similar values, for example on how strongly a statement needs to be supported by empirical evidence. Hence, care must be shown when interpreting the consensus of, for example, technical experts as knowledge (Lacey 2015). A means for avoiding this problem is of course to include broad participation in the assessments. Only if experts represent different areas/disciplines and values, and are able to reach consensus, does it make sense to talk about knowledge-based consensus (Miller 2013). However, the requirement for diversity may face many obstacles in practice, such as lack of time and money to gather different experts.

Often consensus between experts representing a narrow expert base would be interpreted as strong knowledge, even though the criterion of social diversity is not met. For complex issues, dissensus among experts who represent different disciplines/areas and values is likely and could obviously represent more valuable knowledge for the decision-makers in many cases than a consensus perspective among experts having the same type of background.

It is common to distinguish between the following basic types of research and research methods: descriptive vs analytical, applied vs fundamental, quantitative vs qualitative, conceptual vs empirical (Kothari 2004). Most research work in practice is a combination of several of these types. On a more detailed level, a number of methods can be identified, including experiments, surveys, questionnaires, interviews, case studies, observational trials, studies using the Delphi method, simulation, and various statistical methods.

Conceptual research is of special interest in relation to risk analysis and this book, as was mentioned in Section 1.6.4. This type of research relates to some abstract ideas, concepts, theories, etc. and includes one or more of the following elements: identification (for example, a new concept or principle), revision (seeing what has been identified in a different way, for example using alternative frames of reference), delineation (for example, a framework for when to use an assessment approach), summarization (to see the forest for the trees, for example reducing what is known about a matter to a manageable set of contributors), differentiation (for example, that there are several ways of interpreting a probability), integration (to synthesize, amalgamate or harmonize, for example as the unified understanding of risk reflected in the SRA (2015a) Glossary), by advocating (for example, argumentation to justify or support a given conclusion concerning the use of a specific definition or principle), and refuting (for example, argumentation aimed at rebutting a given perspective) (MacInnis 2011). The research is based on creativity, divergent thinking, comparative reasoning, integrative thinking, logic, etc. and makes use of different types of tools, as described in MacInnis (2011): for example, metaphors, questioning of strongly held assumptions, and maps which show relationships between different concepts.

The quality of conceptual research is evaluated similarly to other types of research; see, for example, Yadav (2010), who points to a set of criteria including *exposition* (conceptual clarity and internal consistency), *theory building* (e.g. precision and rationale), *innovativeness, potential impact* and *validity*. Validity can be seen as reflecting the degree to which one is able to conceptualize what one would like to conceptualize. Yadav (2010) uses a different formulation, but it is considered to basically capture the same content. Morse et al. (1996) give four specific criteria related to exposition and theory building, capturing the definition of the concept (is it well-defined?), the characteristics of the concept (are they identified?), the conceptual preconditions and outcomes (are they described and demonstrated?), and the conceptual boundaries (are they delineated?).

Several such formulations of criteria exist for evaluating research, similar to those of Yadev (2010). Common aspects covered are originality, solidness, relevancy and usefulness (see e.g. Aven and Heide 2009).

Conceptual thinking is related to all types of research, also empirical when for example developing hypotheses, or in ethnographic works which build concepts on the basis of observations of people, or in meta-analyses which build on data in the form of individual research papers. Case study research, as discussed by Flyvbjerg (2006), is another illustrating example of how empirical and conceptual research are intertwined. Cases and examples illustrate the thinking and are important in stimulating the creation of ideas and concepts. If no case or example can be derived, it is often a signal that the research ideas are not yet developed.

The starting point for this discussion was that knowledge is understood as justified or warranted beliefs or statements. The above review and analysis point to the fact that this knowledge is mainly generated on the basis of empiricism (data, information, testing) and conceptual analysis and reasoning (theory, models, argumentation). As empiricism is also dependent on conceptual analysis and reasoning, knowledge generation can be seen as founded on conceptual analysis and reasoning, which, in its turn, to a large extent, is built on empirical input.

What is knowledge and in particular scientific knowledge is defined by the knowledge discipline, by the justification processes there defined. Several specific methods are used in this process, but knowledge cannot be restricted to the generation of knowledge through some specific methods, as a method-delineation of knowledge and science can only have temporary validity, as was discussed in Section 2.1.

Evaluation is an integrated part of all types of research, to check whether the concept, method, etc. works as intended or in line with some specified criteria. There are many types of evaluation methods; a distinction is often made between *scientific-experimental models, management-oriented systems models, qualitative/anthropological models, and participant-oriented models* (Trochim 2000). Cost-benefit analysis is a special type of evaluation method. It is commonly used to check whether an approach is cost-effective: the benefits match the costs. The strengths and limitations of this approach are well-known; see, for example, Aven and Renn (2018) and Section 7.1.

3 The risk analysis science

Foundation

This chapter presents and discusses the main features of the risk analysis science, following the basic ideas concerning science described in the previous chapter. The chapter has two main sections. The first gives an overview of the main building blocks for this science, including a list of key pillars or principles linked to the main subject areas of risk analysis: the scientific basis, fundamental concepts, risk assessment, risk perception and communication, risk management and governance, and 'solving real-life risk problems and issues', in line with SRA (2017a). We will come back to many of these pillars and principles in the coming chapters, with rationale and discussion. This section also includes some reflections on the importance of establishing this science. The last main section of the chapter, Section 3.2, discusses how this science generates knowledge. We question: what types of research methods are used in risk analysis?

3.1 THE RISK ANALYSIS SCIENCE – MAIN FEATURES

Remember that risk analysis is here understood as risk understanding, risk assessment, risk characterization, risk communication, risk management, risk governance, and policy relating to risk, in the context of risks which are a concern for individuals, public and private sector organizations, and society at a local, regional, national or global level. A distinction is made between generic risk analysis and applied risk analysis (Figure 3.1):

A. Applied risk analysis: Risk analysis of a specific activity (interpreted in a broad sense, also covering natural phenomena) in the real world, for example an investment, the use of a medical drug, the operation of an

offshore installation, a political decision or globalization. The aim is to support risk knowledge generation and communication, and the handling (management, decision-making) of risk problems and issues.

B. Generic risk analysis: Development of generic risk analysis concepts, theories, frameworks, approaches, principles, methods and models, i.e. development of generic concepts, theories, frameworks, approaches, principles, methods and models to understand, assess, communicate, manage and govern risk.

For A, risk analysis provides input to this risk knowledge generation and communication, and the risk problem tackling, which are commonly multidisciplinary and interdisciplinary activities. Risk analysis is a 'support science' – not the core science in most cases. For example, if we are to study climate change, risk analysis can be useful for characterizing risk, but the fundamental knowledge generation is built on natural sciences.

The B part is genuine risk analysis in the sense that no other fields or sciences address this task on a generic level. Different applications may discuss how to best analyse risk, for example health risk, but these are driven by the goal of solving the practical issues within that application. The B part is, on the other hand, rooted in generic questions and problems, concerning, for example, how to conceptualize and measure risk, how to understand why lay persons' risk perception could differ strongly from professional risk analysis judgements, how to best communicate risk, how to make sense of the precautionary principle, how to best compare benefits and risk, how to make use of cost-benefit analysis in risk analysis, etc. The scientific journals on risk cover papers on such issues, in the same way that statistical journals

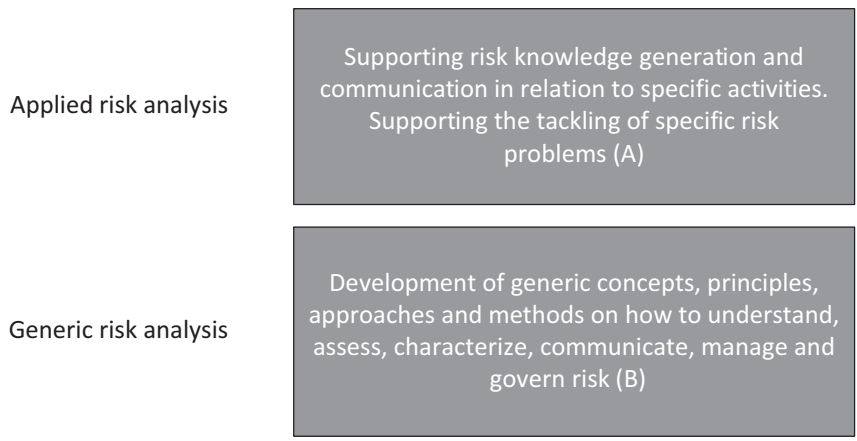


FIGURE 3.1 The two types of risk analysis: applied risk analysis and generic risk analysis (based on Aven 2014a, Aven 2017a, SRA 2017a)

include contributions on statistical concepts and methods. The similarity with statistics is striking. As for risk, we can distinguish between applied and generic statistical analysis:

A1) Applied statistical analysis: statistical analysis of a specific activity to support knowledge generation, communication and management decisions.
B1) Generic statistical analysis: development of generic concepts, theories, frameworks, approaches, principles, methods and models for collecting, analysing, presenting, and interpreting data.

On a structural level, statistics and risk analysis are of the same type. Risk analysis uses statistics but covers many topics not addressed in statistics, as the above examples illustrate.

There is an interaction between A and B: insights from A activities can lead to developments in B, and, of course, findings in B could influence the practical work of A. See Figure 3.2. Developments in other fields, like psychology, statistics and operations research, can also provide useful contributions to risk analysis, directly or adjusted to fit the risk analysis context. Consider, for example, Dennis Lindley, who has conducted ground-breaking work related to uncertainty conceptualization and treatment, of the utmost importance for risk characterization and management (e.g. Lindley 2006).

Every real-life risk analysis performed or every practical guideline for how to carry out risk analyses does not necessarily add anything to the science of risk analysis. They will not be published in a scientific journal. These real-life risk analyses and guidelines should, however, be supported by a science, a risk analysis science, that continuously strives for improvements benefiting the applications.

The risk analysis field generates knowledge according to A and B. The risk analysis science generates *scientific* knowledge according to A and B, where 'scientific' here refers to the most warranted (justified) beliefs or statements that the risk field produces.

As seen from Figure 3.3, risk analysis is influenced by other sciences, and, using the Hansson (2013a) taxonomy, we may refer to nature (natural science), ourselves (psychology and medicine), our societies (social sciences), our own physical constructions (technology and engineering) and our own mental constructions (linguistics, mathematics and philosophy). Applied risk analysis integrates risk analysis knowledge and other sciences, for example to study climate change or medical problems. It is interdisciplinary, as is applied statistics. Generic risk analysis also uses knowledge from other fields, for example probability theory and statistics, but generic risk analysis

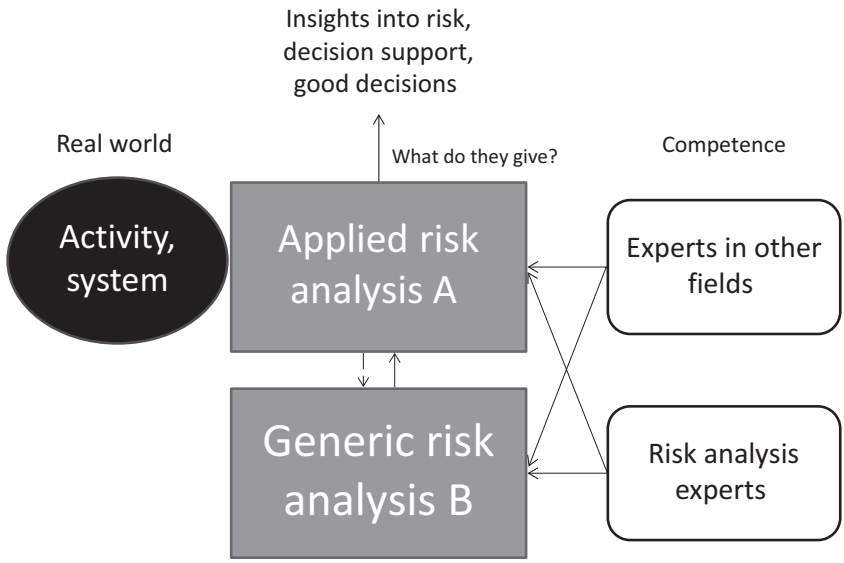


FIGURE 3.2 The model in Figure 3.1, with more detail on competence and interaction (based on Aven 2017a)

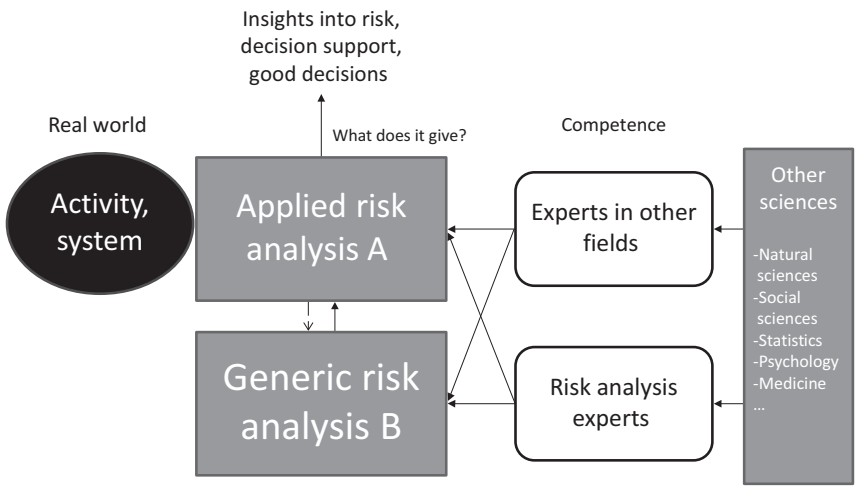


FIGURE 3.3 The model in Figures 3.1 and 3.2, showing how risk analysis is influenced by other sciences

may also be labelled 'our mental constructions', using the science classification system introduced in Section 2.1, in the same way as generic statistics. If we are to include applied risk analysis, 'our mental constructions' would not be sufficient.

Risk analysis is politically neutral in the same way as statistics. It has no view on political issues. Risk analysis can be used to foster growth, sustainability or other goals and visions. The concepts, approaches, principles, methods and models provide support for decision-making, but do not prescribe what policies and decisions are to be made.

It is important to note that the risk science as defined above builds on and extends beyond more specific perspectives, such as the mathematical one commonly discussed in the literature, which is founded on mathematical and probabilistic modelling, subjective probabilities (interpreted in accordance with e.g. Savage (1954) and Ramsey (1931)), and utility theory (e.g. Roberts 1985, Pfanzagl 1968, Bedford and Cooke 2001). Certainly, this perspective and the work conducted within its scope are important and represent essential input to the risk science. However, this science is not limited to this perspective. It is much broader. It includes all concepts, principles, approaches, theories, methods and models for understanding, assessing, communicating, managing and governing risk.

As formulated by Bedford and Cooke (2001, p. 20), a mathematical representation of uncertainty is founded on axioms, interpretations and measurement procedures. For probability, these criteria are met but, when aiming at properly characterizing risk and uncertainties in a practical setting, we need to see beyond the mathematical framework and also apply qualitative judgements. For example, the current book argues that the concept of subjective probability should not be based on frames and interpretations as referred to above (e.g. Ramsey, Savage), as these have an unfortunate mix of uncertainty judgements and value judgements. Moreover, when subjective probabilities are used to describe risk or uncertainties, there is a need to address the strength of the knowledge supporting these. This cannot be done mathematically. It is not covered by the mathematical theory referred to. It is not a part of the foundations addressed in this mathematical theory, but it is relevant for practical risk and uncertainty management. Finally, the potential for surprises is highly relevant for risk and uncertainty management, but it is not an aspect of the mathematical perspective referred to above. The coming chapters will give further details and other examples.

3.1.1 Basic principles

In this section, a set of pillars (principles) for the field and science of risk analysis is presented, covering the scientific basis, fundamental concepts, risk assessment, risk perception and communication, risk management and governance, and 'solving real risk problems and issues', in line with recent risk analysis research and guidance (Aven 2018a, SRA 2017b). The pillars will be discussed in more detail in the coming chapters.

The scientific basis

1. The risk science covers risk understanding, risk assessment, risk characterization, risk communication, risk management, risk governance, and policy relating to risk, in the context of risks which are a concern for individuals, public and private sector organizations, and society at a local, regional, national or global level. A distinction is made between generic risk analysis and applied risk analysis as defined above.
2. The knowledge production of the risk analysis field covers:
    i. knowledge production of type B, generated by the risk analysis field/discipline (all relevant journals, papers, researchers, research groups and societies, etc.). It covers generic concepts, theories, frameworks, approaches, principles, methods and models to analyse risk (understand, assess, communicate, manage and govern risk)
    ii. knowledge production of type A, covering risk knowledge for specific activities in the real world, generated by risk analysis and risk analysis professionals (analysts, researchers), together with other fields/disciplines and professionals.

The knowledge production of the *risk analysis science* covers the same components, with knowledge replaced by scientific knowledge: the most warranted (justified) beliefs or statements that the risk field produces.

To perform the type A analysis, different approaches are used and issues raised, including (SRA 2017a):

a) Descriptive analysis: what has happened in terms of losses, failures, etc.? What do the data indicate is (not) worth worrying about? What has changed that seems worth worrying about?
b) Predictive analysis: what will happen if a specific activity is realized? What might go wrong? Why and how might it go wrong? What are the consequences? How bad is it? What will happen if we (do not) intervene? How soon, with what consequences?

Causal analysis: What will happen if we intervene in different ways?

c) Prescriptive analysis and decision optimization/management: what should we do next, given the resources, risk, uncertainties, constraints and other concerns? Who should do what? Who should use what decision rules? What are intolerable or unacceptable risks? How can the public participate? How to be prepared in case of an event? How to build robust and resilient systems?
d) Communication: who should say what to whom? How?
e) How are perceptual aspects like fear influencing risk judgements?

f) Evaluation analysis: how well is the risk analysis working? What have the consequences of our actions and policies actually been?
g) Learning analysis: how might we do better? What should we try next, and for how long? When should we stop exploring and commit to a policy?
h) Collaborative analysis: how might we do better together?

The knowledge production of type B covers the development of concepts, principles, methods, models, etc. for these activities.

The five-step model for the knowledge process

A model for the knowledge process is presented by Hansson and Aven (2014), comprising the following five steps: evidence, knowledge base, broad risk evaluation, decision-maker's review and judgement, and decision (see also Figure 5.8 in Section 5.5.3). The last three steps are, to a large extent, value-based. Many risk assessment studies stemming from various scientific committees perform the risk evaluation function. The decision-maker's review extends the considerations of the scientists by combining the risk information he or she has received with information from other sources and on other topics. This model applies primarily to the A type of knowledge, but it is also applicable to the B part, as will be discussed in Section 3.1.4.

Concepts

3. Risk is the mental concept that exists when considering an activity in the future (even if this risk is not measured or characterized). It comprises two main features: i) values at stake (consequences with respect to something that humans value) and ii) uncertainties (what will the consequences be?). Alternative ways of explicitly formulating this idea exist (see Section 4.1).
4. Measuring and characterizing risk include representing, modelling or expressing these two features. The risk measurements or characterizations can be intersubjective but are not objective or independent of the assessor.
5. A probability model is used to represent variation in huge populations of similar units. It is often referred to as aleatory or stochastic uncertainty (this is an unfortunate terminology, as the concept reflects variation and not uncertainty). A probability model is a set of frequentist probabilities. A frequentist probability $P_f(A)$ of an event A expresses the fraction of times event A occurs when considering an infinite population of situations or scenarios similar to the one analysed. Probability models and frequentist probabilities need to be justified. In many cases, they cannot be meaningfully defined. Usually $P_f(A)$ is unknown, and we are led to estimation and uncertainty assessment of $P_f(A)$. It is essential to distinguish between the underlying concept $P_f(A)$, on the one hand, and

estimators/estimates and uncertainty judgements of $P_f(A)$, on the other. (In a purely Bayesian framework, the term 'chance' is often used instead of frequentist probability – it refers to the limiting fraction of binary, exchangeable random quantities.)

6. Probability, including interval probability, is a tool for expressing the assessor's uncertainty and beliefs about unknown events and quantities (including parameters of probability models). A probability is interpreted with reference to a standard: if, for example, a probability of 0.15 is assigned for an event A, the assessor has the same uncertainty (degree of belief) that A will occur as randomly drawing a red ball out of an urn which comprises 100 balls of which 15 are red. In the case of a probability interval, the assessor is not willing to be more precise than the interval specifies. Hence, if an interval [0.1, 0.2] is specified, the assessor is not willing to be more precise than expressing that his/her degree of belief that the event will occur is at least as high the degree of belief in drawing a specific ball from an urn comprising 10 balls, and lower or equal to the degree of belief in randomly drawing a specific ball from an urn comprising five balls. Alternatively, the interval corresponds to randomly drawing a red ball out of an urn comprising 100 balls, where 10 to 20 are red – the exact number is not specified. Other ways of interpreting probability exist, but these are not in general considered suitable for risk analysis (see Aven and Reniers 2013).
7. A probability (interval probability) for an event A is based on some knowledge K. We write P(A|K). This knowledge needs to be considered, together with the probability (probability interval), to provide a full representation or characterization of the uncertainties of the unknown events and quantities. Such considerations can be based on judgements of the strength of this knowledge, addressing issues like assumptions made, the amount and relevancy of supporting data and information, agreement between experts, the understanding of the phenomena studied, degree of model accuracy and the degree to which this knowledge has been examined (for example, with respect to signals and warnings, knowledge 'gaps', etc.)
8. A model g is a simplified representation of an aspect of the world. If Z is the quantity to be modelled, the difference g-Z is the model error. Uncertainty about this error is referred to as model uncertainty.
9. Other risk-related concepts build on the same logic: a qualitative broad definition of the concept and ways of measuring or characterizing it, reflecting uncertainties in a similar way and building on an understanding of risk, as described above. The SRA (2015a) Glossary represents a list of current definitions in line with this thinking: see also Appendix A.

Risk assessment

10. Risk assessment is the systematic process for identifying risk sources, threats, hazards and opportunities; understanding how these can occur and what their consequences can be; representing and expressing uncertainties and risk; and determining the significance of the risk using relevant criteria. A risk assessment aims to produce knowledge of type A. The B type of knowledge is related to producing concepts, principles, models, methods, etc. for this purpose (to produce the A knowledge).
11. Probability theory and other frameworks are used for representing, modelling and treating variation and uncertainties; statistics and Bayesian analysis provide basic tools of risk assessment.
12. The scientific quality of a risk assessment can be judged through at least two main perspectives:

    a) The analyst and scientist perspective: the degree to which some basic scientific requirements are met, such as (Aven and Heide 2009):

        i. The work is *solid* in the sense that it is in compliance with all rules, assumptions, limitations or constraints introduced, and the basis for all choices, judgements etc. given is clear and logical, and, finally, the principles, methods and models are subject to order and system, to ensure that critiques can be raised and that it is comprehensible. All analysis approaches and methods used are properly justified.
        ii. The analysis is *relevant and useful* – it contributes to a development within the disciplines it concerns, and it is useful with a view to solving the problem it concerns or with a view to further development, in order to solve the problem it concerns.
        iii. The assessment and results are *reliable* and *valid*. While reliability is concerned with the consistency of the 'measuring instrument' (analysts, experts, methods, procedures), validity is concerned with the success at 'measuring' what one sets out to 'measure' in the analysis.
        iv. A key aspect to be considered in relation to validity is the degree to which the knowledge and lack of knowledge have been properly addressed.
        v. The analysis team has strong experience and competence as regards both the system/activity studied and as risk analysts (scientists).

    b) The decision-maker's (and other stakeholders') perspective: the confidence he/she has in the assessment and its results and findings. This confidence will depend on many factors, including:

i. The analysts' and scientists' judgements in relation to a), for example the analysts' and scientists' judgement of the strength of knowledge supporting the risk results and risk related to deviations from the assumptions made.
ii. The decision-maker's own assessment of such issues.
iii. The decision-maker's understanding of what the risk assessment actually produces. The decision-maker can, for example, to a varying degree, be aware of the fact that the risk assessment results are dependent on a background knowledge which can be more or less strong and include erroneous beliefs.
iv. How the decision-maker judges the competence of the analysts and scientists.

The confidence is only one aspect for the decision-maker to take into account when making a decision concerning risk (see items 21–5).

Risk perception and communication

13. Risk perception refers to a person's subjective judgement or appraisal of risk, which can involve social, cultural and psychological factors. The A type of knowledge relates here to how risk is perceived in real-life settings, how affect and trust influence people's risk perception and behaviour. The B type of knowledge covers the development of concepts, theories, approaches, methods, etc. for producing the A type of knowledge.
14. Risk perceptions need to be carefully considered and incorporated into risk management, as they will influence how people respond to the risks and subsequent management efforts. Risk perception studies are important for (i) identifying concerns but not necessarily for measuring their potential impacts and (ii) for providing value judgement with respect to unavoidable trade-offs in the case of conflicting values or objectives.
15. Risk communication covers exchange or sharing of risk-related data, information and knowledge between and among different target groups (such as regulators, stakeholders, consumers, media and the general public). The A type of knowledge relates to how this communication is actually conducted, whereas the B type of knowledge covers the development of concepts, theories, approaches, methods, etc. for conducting the risk communication.
16. Risk communication is multi-directional and includes both formal and informal messages and purposeful and unintentional ones. In today's super-mediated environment, risk professionals must also recognize that any risk message they seek to communicate is likely to be competing with multiple, conflicting messages from unofficial sources.

17. Successful risk communication requires an understanding of the target audience, including the best means for reaching the audience: a credible or trusted source and a message that has ideally been pre-tested to ensure its effectiveness. Those seeking to develop and test risk messages employ a host of methods, including surveys, focus groups, interviews and experiments.
18. A prerequisite for successful risk communication is high-quality scientific risk analysis.
19. With few exceptions, such as proprietary information or that which may damage public security, risk professionals should seek an open, transparent and timely risk communication policy. Such a policy not only demonstrates respect for the target audiences and ensures they have the information they need to take risk mitigation actions, if necessary, but it can also help to ensure the perceived trustworthiness and legitimacy of the sources.

Risk management and governance

20. Risk management covers all measures and activities carried out to manage and govern risk, balancing developments and exploring opportunities, on the one hand, and avoiding losses, accidents and disasters, on the other. The A type of knowledge relates to how this management is actually conducted, whereas the B type of knowledge covers the development of concepts, theories, approaches, methods, etc. for conducting the risk management.
21. Risk assessments inform decision-makers; the assessments do not prescribe what to do – even in the case that the decision-maker has a high level of confidence in the risk assessment. The decision-makers need to take into account limitations of the risk assessments, as well as concerns and issues not addressed in the risk assessments. Any quantitative risk assessment is based on some knowledge (justified beliefs), which could be more or less strong and also wrong. The decision-makers need to take this into account when making their decision.
22. Three major strategies are commonly used to manage risk: risk-informed, using risk assessments, cautionary/precautionary and discursive strategies. In most cases, the appropriate strategy would be a mixture of these three strategies.
23. The cautionary and precautionary principles have an important role to play in risk management, to ensure that proper weight is given to uncertainties in the decision-making. Robustness and resilience are examples of cautionary thinking. The concepts reflect the ability of a system or organization to maintain or regain a normal state, given a change, disturbance or stress.

24. Risk acceptance and tolerability should not be based on the judgements of probability alone, as risk is more than probability, and concerns other than risk need in general to be considered when making decisions relating to risk. Pure probability-based risk acceptance (tolerability) criteria should consequently not be used.
25. Cost-benefit type analyses need to be supported by risk assessments, to provide adequate decision support, as these analyses are based on expected values, which, to a large extent, ignore risks and uncertainties.

Solving real risk problems and issues

26. There are many challenges and issues related to solving real risk problems in practice (which are usually multidisciplinary and interdisciplinary in their form), by integrating theories and methods from risk assessment, risk perception, risk communication and risk management, as well as from other fields/disciplines. The A type of knowledge here relates to how such problems are actually solved, whereas the B type of knowledge covers the development of concepts, theories, approaches, methods, etc. for how to solve them.

3.1.2 Core subjects of risk analysis

In Appendix B, a list of core subjects of the risk analysis field and science is presented. The list is based on work carried out by the Society for Risk Analysis (SRA 2017a).

For any field, there will be a continuous discussion on what represents its core. Consider, for example, statistics. If we study basic courses and textbooks in this field, we observe some common topics and a number of issues that are covered by some but not others. Yet, no one would question the usefulness of having defined a core that all students should cover in a basic course in statistics. The same should be the case for the risk analysis field. As for statistics, we would use examples to illustrate the concepts, theories, principles and methods. As it is the concepts, theories, principles and methods that are the key in this respect, these examples should be simple and illustrative. An engineer who is to learn about statistics will not benefit much from detailed studies in statistical analysis related to, for example, finance or health, but simple educational examples from these areas of applications could be useful.

We would have the same situation for risk analysis. For an engineer who is to study risk, simple examples from various applications can be instructive, but, if they are too detailed, they will not contribute to meeting the aim of the study.

An example of a topic listed in this subject list is probability. The topic of probability is not only ‘owned’ by the risk analysis field; however, risk

analysis is the main and only field for the understanding and use of probability in a risk analysis context, which is the scope of this book.

We refer to SRA (2017a) and Appendix B for further details. The above pillars for the risk analysis science are in line with these core subjects. Both SRA (2017a) and the present pillars are consistent with the SRA (2015a) Glossary.

3.1.3 Implications

If risk analysis can be developed and broadly recognized as a distinct science, it will have some implications for science in general and risk problem solving in particular. This section provides some reflections on these implications.

Unity on terminology and basic principles

Certainly, it would mean that the risk analysis field would obtain some unity when it comes to terminology. This is highly welcomed, as all disciplines and sciences need a common platform on basic definitions and understanding of key concepts. Currently, the situation is rather chaotic. Terminology is important, as it mirrors the underlying thinking. For example, the way risk is conceptualized strongly influences how risk is to be understood, assessed, characterized, communicated and managed. According to items 3 and 4, risk captures two main features – values (consequences for something humans value) and uncertainties – and any risk metric used then needs to be seen in relation to how well it reflects these features. Surely, using an expected value as a risk metric would then, in most cases, be a very poor risk characterization. Decision-makers could be seriously misguided if giving weight to this metric. Today, we see a number of applications and publications on risk, starting with risk actually being defined as expected value, despite the limitations of this metric. With a risk analysis science working as intended, such a practice is likely to change, and broader ways of characterizing risk, reflecting that probability and other quantitative ways of measuring or describing risk are just tools and have limitations, would be adopted. A key point is that the knowledge that the metrics are based on also needs to be considered in relation to risk, as the knowledge could be more or less strong and also wrong.

Today, we see probability being used in risk analysis without any explanation of what it means. The result is poor science – a lack of precision, which easily leads to inaccuracies and erroneous inference. Adopting the above pillars, the analysts and researchers need to clarify whether probability is used to represent variation or the assessor's uncertainty or degree of belief, and how to make appropriate interpretations of the term in these two situations.

A stronger guidance for applications

Consider some scientists studying a specific phenomenon, for example the occurrence of a disease, an earthquake, a process fire or the realization of a comprehensive project. Their work is, to a large extent, about risk. To support their work, they need to conceptualize risk and characterize it. They look for guidance provided by their discipline (for example medicine), relevant standards and perhaps also some scientific literature on the topic, for example books addressing risk related to this phenomenon. Based on this, the scientists may conclude that risk should be conceptualized as a probability linked to defined events or loss categories, or as a statistical expected value determined as the product of loss and probability, summed over all loss values. These scientists have their main competences in their discipline (medicine, natural science, engineering, etc.) but not in risk. They are dependent on others to properly conduct the work related to risk. The discipline-oriented guidance provides some input, but it is not enough. They should consult the field and science which has risk as the main subject area: namely, risk analysis. When studying risk analysis, the scientists will be challenged in their perspective. First, they are stimulated to clarify what probability means in this context as discussed above. Secondly, they will be challenged in the way risk is conceptualized. Probability is just a tool for measuring or characterizing the uncertainties, but it is basic knowledge from measurement theory that we should separate the concept and how it is measured. This is also the case with risk. If probability is used in the definition of risk, such a separation is lost (interpreting probability as a measure of uncertainty). The result is often a lack of understanding and acknowledgement of the limitations of the risk metrics used. Risk is more than that which is captured by the probabilistic quantities.

When a risk problem is addressed for the A type of knowledge production, for example in climate change research, the risk analysis science as described here provides strong guidance on how to deal with risk and uncertainties. Current practice has shown that there is a substantial potential for improvement (Aven and Renn 2015); see also discussion in coming chapters. Another example is the Global Risk Reports by the World Economic Forum (refer to Section 1.2), which present a 'risk landscape', using the dimensions of likelihood and impact, developed from a survey of a large number of members of the World Economic Forum's global multi-stakeholder community. Starting from a risk analysis science as outlined here, this risk landscape would have been quite different from the one now presented. The overall judgements of what constitute high risks in our society would also then be affected. The example will be discussed in more detail later; see Section 4.2.4.

A better balance between confidence and humility

A science based on the above pillars will mean a humbler attitude towards science and the 'truth' than often seen today. The knowledge generation is about justified beliefs, not justified *true* beliefs. It does not mean that the justifications cannot lead to truth claims being made in a practical setting – as, for example, the risk related to smoking. As a science, we will, however, always have to underline the justification and the knowledge supporting the claims. The history of science should have taught us that surprises may occur. What we believed so strongly could turn out to be wrong, or more reflections are needed to provide a proper characterization of the problem. As in so many aspects of life, the issue is really about finding the proper balance between confidence (believing in something) and being humble and open, so that we can improve and learn more. Compared to what we often see today, the science promoted here adjusts this balance somewhat to the humble side, while still giving due weight to the confidence part. The motivation for the change is simply to reflect all the aspects in the justification process in a fair and balanced way, giving due consideration to the limitations of the tools used.

More risk analysis research

A distinct risk analysis science is likely to lead to more and stronger research on risk analysis. Starting from the basic pillars, the research can reach a higher level. Today, too many analysts and scientists start basically from scratch when they perform risk research, using different principles and methods, many of which the B knowledge has shown suffer from severe weaknesses and should not be used. Accepting the pillars would also lead to new research topics, an illustration being the knowledge aspect of risk, which has not been given much attention in the risk analysis literature beyond probability and the related tools used to quantify uncertainty. Moreover, a distinct risk analysis science would lead to increased focus on the B type of knowledge generation, as the core of the field is so strongly linked to such developments. If we are to solve real-life risk problems, it is essential to have a strong B part, giving proper guidance on how to understand, assess, characterize, communicate and manage risk. As for all sciences, there is no static condition in the sense that the pillars are not scrutinized. There is no conflict in building the science on a platform as described above, while, at the same time, doing research, exploring and questioning the features and basic ideas of this platform, with the aim of improving it and making it even stronger. On the contrary, without such research, the field and science will not properly develop. It is again about balancing confidence and humility.

As risk analysis is not considered a distinct field or science in many research funding schemes, applications in risk analysis need to be justified, given their role of solving specific risk problems. This makes it difficult to obtain funding for the generic part of risk analysis, and the risk analysis experts' main task easily becomes that of serving others in solving their problems, whether in medicine, engineering or finance. A broadly accepted risk analysis science would hopefully change this situation.

See also related comments in the Preface.

3.1.4 Summary and some additional remarks

Risk issues are growing in our society, and the dialogue about them and their treatment is not trivial. The risk analysis field and science can and should play an important role in framing and guiding the understanding and handling of these risk issues. To some extent, risk analysis is doing this today, but there is a potential for improvement, as argued for above.

The previous sections have presented the core basis for a risk analysis science to exist as a science in itself. This science is referred to as an emerging science, as it is rapidly developing and is not yet broadly recognized as a distinct science. The present book argues that risk analysis is a distinct science in the same way that statistics is. It distinguishes between two different types of knowledge generation for risk analysis: A) risk knowledge related to an activity in the real world, and B) knowledge on concepts, theories, frameworks, methods, etc. to understand, assess, characterize, communicate and (in a broad sense) manage risk. For the B type, the risk analysis science is analogous to the corresponding science of, for example, statistics. For the A type, the risk analysis science supports the knowledge generation – as well as the risk communication and management – and, with suitable support from B, this type may also produce scientific knowledge. Again, a comparison can be made with statistics. To obtain a broader acceptance of risk analysis as a distinct science, it is essential that organizations like SRA intensify their work on strengthening the foundation of the risk analysis field.

Risk analysis builds on many principles, approaches and methods. These are not static, but there should be little discussion about the usefulness of the traditional scientific method when data can be observed. However, the science of risk analysis extends beyond such principles, approaches and methods. The traditional scientific method, for example, is not applicable in many cases, such as when the uncertainties are large. Risk assessment does not have any explanatory power in such situations – accurate predictions cannot be made. Yet, the traditional scientific method is considered a useful tool in some cases, when it can be justified. For the risk analysis science, a broader basis is, however, established as knowledge generation. And also, in the case

of large uncertainties, such knowledge is generated: knowledge on how to conceptualize, assess, characterize, communicate and manage risk.

The five-step model for the knowledge process, with focus on the generic B knowledge

Section 3.1.1 referred to a model for the knowledge process, comprising five steps: evidence, knowledge base, broad risk evaluation, decision-maker's review and judgement, and decision (see also Figure 5.8 in Section 5.5.3). The decision-maker's confidence in the risk analysis (in particular the risk assessment) process and findings, as highlighted in Section 3.1.1, is important for how the risk analysis influences the decision, but the decision-maker also needs to take into account other types of factors not normally reflected in the confidence judgements, such as costs, reputation and strategical issues. This model was originally developed for type A knowledge production, but it also works for B knowledge. The evidence is published in papers and presented at conferences on the topic considered, for example how to conceptualize risk. All contributions on the topic add to the knowledge base on this topic, which the relevant group of experts and scientists take as given in further research and analysis in the field. Then a broad evaluation is conducted. It could be a process, run for example by a professional society, like Society for Risk Analysis, trying to conclude what is the essential scientific knowledge generated by all these contributions on the topic considered. Currently, no official institutions exist that can conduct such evaluations on behalf of the scientific environment of risk analysis, and it is obvious that any such institution and their findings would be subject to a lot of discussion. Yet, as a science, risk analysis needs to conduct such work to be able to provide suitable guidance for the applications of risk analysis. The fourth step involves a scientist or scientist team that is informed by this evaluation but also takes into account other aspects, for example their own research on the topic considered. At the end, the scientist (team) makes a choice on what is the most suitable concept, approach or method.

The key subjects of risk analysis

The pillars of the risk analysis field, as described in Section 3.1.1, provide input on what the key subjects of risk analysis are, which would be covered by courses in risk analyses; see also Section 3.1.2 and Appendix B. The pillars represent the result of an evaluation, using the above model for knowledge generation. Certainly, this evaluation has strong elements of value judgements. The same could be said for a specific course implementation of the subject list, although it is more value-neutral when just listing the topics to be included, such as:

> The probability (likelihood) concept. Variation and probability models. Frequencies. Understanding and using subjective probabilities to reflect epistemic uncertainties and degrees of belief. Why the use of probability to represent uncertainties? Bayesian analysis. Generalizations of probability theory. Interval (imprecise) probabilities and related 'non-probabilistic' characterisations and metrics.
>
> (SRA 2017a; see Appendix B)

Challenges related to defining the pillars

There are many challenges related to the foundation and applications of the concepts, approaches and methods referred to in Section 3.1.1. For example, how to best represent the knowledge available when characterizing risk is an important research question, and it is challenging from a theoretical and a practical point of view to use interval (imprecise) probabilities. Yet, relevant guidance exists on how to best meet these challenges.

It is commonly argued that the way in which risk is conceptualized and analysed always needs to be adapted to the situation at hand – different situations call for different solutions. However, such a perspective is easily refuted. The concept of risk conceptualizes ideas that apply to all types of applications. In the same way, we can discuss the meaning of the precautionary principle and how to use it, on a generic level, and so on. The scientific literature includes a large number of papers of this form, giving input to the B type of research. This research will then provide a basis for the development of the tailor-made methods, models, etc. to be used in different applications.

In Section 3.1.1, basic requirements were formulated for ensuring the quality of a risk assessment and the related decision-maker's confidence. Similar types of requirements can also be formulated for other areas like risk perception or risk communication studies. The quality aspects highlighted for risk assessment are, to a large extent, generic requirements applicable to any type of research. The reliability and validity can also be transferred to other topics. Adjusted interpretations must, however, be given, to make these concepts meaningful for specific use.

3.2 HOW THE RISK ANALYSIS SCIENCE GENERATES KNOWLEDGE (RESEARCH METHODS)

This section discusses research methods related to risk analysis's two main categories of knowledge generation, as presented in Section 3.1.1. Of particular interest is the type B knowledge, as it has a normative dimension;

we seek the best concepts, principles, theories, frameworks, approaches, methods and models and through this are able to provide recommendations on the concepts that should be used. For brevity, we will refer to this category as knowledge generation related to concepts for analysing risk or conceptual research in risk analysis.

But what is the 'best'? For example, is there a best definition of risk? There is obviously not a universal 'correct' definition; hence, the research is not about truth claims, as in A, where we could, for instance, aim to prove that a type of chemical is dangerous to human health. For B, the challenge is rather to develop the argumentation that supports a specific concept and to judge the strengths of this argumentation, in relation to some suitable criteria. Defining which criteria to apply is an important task within this research.

To a large extent, the A research category is about understanding the 'world', and established research methods exist, including the traditional 'scientific method' (see Section 2.3), using observations to establish accurate theories and models (empiricism). Statistical inference provides the common framework for carrying out this method. Risk analysis supports this knowledge generation, by using suitable risk analysis concepts and by interacting with other fields.

Using some illustrating examples, the main aim of this section is to demonstrate the importance of conceptual research in risk analysis. First, in Sections 3.2.1 and 3.2.2, research methods relevant for the A and B categories, respectively, are discussed, using several examples addressing different types of risk analysis issues. Section 3.2.3 follows up these sections with a broad discussion of the findings made, and Section 3.2.4 provides some conclusions.

3.2.1 Core research methods of risk analysis – type B

This section discusses research methods specifically directed at knowledge generation on risk analysis concepts.

As mentioned in Section 2.3, it is common to distinguish between the following basic types of research and research methods: descriptive vs analytical, applied vs fundamental, quantitative vs qualitative, conceptual vs empirical (Kothari 2004, Trochim 2000). Most research work in practice is a combination of several of these types. Using these categorizations, we can quickly conclude that the relevant research for the B type is mainly fundamental and analytical, rather than applied and descriptive. Specific applications and descriptive work can provide input to the B research, but application and description are not at the core of the research. Furthermore, it is clear that B research can be both quantitative and qualitative, and conceptual and empirical. To explain this in more detail, two illustrative example cases will be considered, the development of the following two concepts:

a) The IRGC risk governance framework (IRGC 2005)
b) The antifragility concept by Taleb (2012)

The issue to be discussed is what type of research methods to use for these developments, when making a thought-construction, moving back in time to their origin. The answer is that conceptual research is the best way to characterize this research. The research is also founded on empiricism, as will be explained in more detail below. Let us first consider example a.

The IRGC risk governance framework

The IRGC risk governance concept was developed under the leadership of Professor Ortwin Renn and is founded on a number of publications, including the IRGC (2005) White Paper on risk governance and the monograph by Renn (2008); refer to Section 1.6. Included in this development, several more specific new concepts were introduced, for example the classification of simple, complex, uncertain and ambiguous risk problems. Also, a new way of defining and understanding risk has been developed (Aven and Renn 2010). The motivation for the new governance framework was an acknowledgement of the need to broaden the risk thinking and approaches in cases with many actors and to meet the new challenges of our time (such as globalization and the increasing complexity of policy issues), as the prevailing mindset and methods were very much based on narrow perspectives using probabilistic risk assessments not suitable for these types of challenges (van Asselt and Renn 2011, Pierre and Peters 2000, Walls et al. 2005).

The research conducted is a combination of conceptual and empirical work. It is empirical in the sense that the recognition of the problem is based on reviewing the then current situation, how risk analyses were typically conducted and how these were meeting society's needs (see IRGC 2005 and its appendix A). This empirical analysis does not aim to be all-inclusive, covering all types of applications and problems, but broad and detailed enough to provide a sufficiently strong support for the conclusion that the prevailing thinking and approaches can be improved by new concepts.

Next, the research work aims at developing the new concept: here, the new risk governance framework. It is a process with one or more features like identification, revision, delineation, summarization, differentiation, integration, advocating and refuting (MacInnis 2011), and using different types of thinking (creativity, divergent thinking, comparative reasoning, integrative thinking, logic, etc.) and tools; refer to Section 2.3. To illustrate, the research uses delineation, summarization, differentiation and advocating, when pointing to suitable risk management strategies for different categories of risk problems. This is mainly conceptual research, founded on reasoning and argumentation.

One example of the types of thinking involved is integrative thinking, in relation to developing a suitable definition of risk to meet the needs of the new framework. An integrative thinking process is a type of thinking which per definition reflects a strong "ability to face constructively the tension of opposing ideas and instead of choosing one at the expense of the other, generate a creative resolution of the tension in the form of a new idea that contains elements of the opposing ideas but is superior to each" (Martin 2009, p. 15). In this case, it recognized that there are several different definitions of 'risk', which can be considered to create tension. However, integrative thinking makes the researchers see beyond these definitions – it utilizes the opposing ideas to obtain a new and higher level of understanding, as also discussed in Aven (2016a).

Refuting is an integral part of the conceptual analysis. Arguing for a concept normally goes in parallel with countering alternatives. In the case of justifying a suitable risk concept supporting the governance framework, it is argued that, for example, expected values and probability-based definitions of risk will not be able to serve the purpose of the framework (Aven and Renn 2010).

As mentioned in Section 2.3, the quality of this type of research is evaluated through common criteria, such as conceptual clarity, internal consistency, precision, rationale, innovativeness, potential impact and validity (see e.g. Morse et al. 1996, Yadav 2010, Aven and Heide 2009). The scientific research process with peer-review of papers is one key check that the work meets such criteria. The problems with this type of evaluation are well-known, yet it is commonly considered the best we have, and it constitutes a pillar for knowledge generation within each discipline. The IRGC framework with its many facets has been extensively published in the scientific literature, and it has been shown to work well in practice – it is valid in that sense. Nonetheless, there are always issues that can be discussed. Continuous evaluation of the concept helps further develop it.

The evaluation of the IRGC framework has been carried out by reviewing and discussing the fundamental theoretical pillars, through applications of the framework, as well as workshops, with both users of the framework and academics present. In evaluation research, the aim is to provide knowledge about how the concept works in relation to its purpose or some defined criteria, what the challenges are and how it can be improved. The research is thus a combination of conceptual and empirical work.

The antifragility concept

Nassib Taleb introduced the concept of antifragility in Taleb (2012). His work has been followed up by many papers providing applications, as well as further theoretical analysis of the concept; see for example Verhulsta

(2014) and Aven (2015a). The basic idea is that some variation, stress and uncertainties are necessary to obtain high performance: not only being resilient but learning from the changes and events occurring and improving.

The development of the antifragility concept very much involves the same type of research approaches and methods as the IRGC framework discussed in the previous section, and there is no need to repeat the discussion: the work is mainly conceptual but has also a basis in empiricism. An observation is, however, in order. The initial work presented in Taleb (2012) is not a research book as such – it does not meet the quality criteria of solidness and conceptual clarity. Yet, the development of the concept can be viewed as research, as it provides new knowledge. For example, Aven (2015a) states that the concept "adds an important contribution to the current practice of risk analysis by its focus on the dynamic aspects of risk and performance, and the necessity of some variation, uncertainties, and risk to achieve improvements and high performance at later stages". The point being made is that a work can be classified as research, despite not necessarily meeting the quality requirements specified by scientific journals. The follow-up papers, as referred to above, have further developed the concept and presented research to frame and give substance to Taleb's initial ideas.

3.2.2 Core research methods of risk analysis – type A

The question now is: what type of research methods are to be used for generating risk knowledge related to real-world activities, for example the climate, the operation of a process plant or the use of a medical drug - the A type, as defined in Section 3.1?

Using the main research categories referred to in the introduction of this Section 3.2, it is immediately clear that the A type is applied and not fundamental; it can be descriptive, quantitative or qualitative, and empirical, and there will always be a conceptual part.

Five examples will be used to illustrate the core research methods of type A, as well as some links to the B type of research.

Using the IRGC framework in a specific case (Barents Sea)

In Aven and Renn (2012), risk management and risk governance, with respect to petroleum operations in the Barents Sea area (including the Lofoten area), are studied, using the IRGC framework as a reference. This area is considered environmentally vulnerable. The authors discuss the extent to which this framework provides valuable insights for and assistance to the decision-maker – the Norwegian Government – and other stakeholders (including the industry and NGOs). In the study, three main questions were raised,

concerning: i) the use of evidence-based risk assessments, ii) the precautionary principle and iii) the justification for judgements about tolerating, accepting or rejecting the petroleum activities.

The study demonstrates that the IRGC framework has the ability to identify issues and deficits in governmental processes of this type, and it provides guidance on how to tackle risk problems. As such, the work is part of the B type of research, evaluating whether the framework functions as intended. Several other historic cases are reported in Renn and Walker (2008). However, the A type of research does not concern the suitability of the IRGC framework but the knowledge gained concerning the governmental processes. The research concluded, in line with the findings of Renn and Walker (2008), that the risk management and governance failed in several ways and the problems could mainly be "traced to an inadequate handling of the frames that characterize the plurality of perspectives in a modern democratic society and the lack of transparency for the trade-offs between risk and benefits in the phase of evaluation" (Aven and Renn 2012).

The authors differentiated between three camps:

> I Political parties to the left and partly in the moderate left centre in conjunction with environmental NGOs: They have a focus on the environmental and social values at stake and they find the risk and uncertainties to be unacceptable (the point is made that we cannot rule out the possibility that a disaster will happen).
>
> II Parties in the moderately right centre of the political spectrum: They would like to have more information before making a decision. They believe in the principle that one can balance benefits and risks but are unsure whether the balance will result in benefits outweighing the risks or vice versa.
>
> III Parties to the right, in conjunction with industry, that believe in the legitimacy of balancing pros and cons in a systematic way and that are convinced that such balancing would result in a judgment that the economic benefits outweigh the environmental and social risks.
>
> (Aven and Renn 2012)

By relating these camps to issues i–iii mentioned above, insights are obtained. For example, for camp I, the actual assessments on risk and cost-benefit are not of interest, as they reject the idea that that the vulnerabilities can be traded off against economic benefits in this case. The precautionary principle was referred to; however, their judgements were probably more about applying the more general cautionary principle, which states that caution

should be the ruling principle in the case of risk and uncertainties. The camp I stand was not really about scientific uncertainties, such as the precautionary principle is built on, but the fact that uncertainties exist: an oil spill could happen, and the result could be severe environmental damage. Refer to Section 7.3.

These are merely illustrations to show how the research generates A type of knowledge concerning the actual risk management and governance in the Barents Sea area. Returning to the research features for conceptual analysis, this Barents Sea research makes use of all these, as illustrated in the following:

- identification – for example, the work identifies which fundamental risk management and governance principles are relevant in the particular case and which are actually referred to
- revision – for example, the work argues that, instead of referring to the precautionary principle, the cautionary principle should be highlighted
- delineation – for example, the study restricts attention to the issue of petroleum operations in specific areas and in a specific period of time
- summarization – for example, the study represents the views and perspectives on the issue of the three camps only
- differentiation – for example, the work differentiates between these three camps.
- integration – for example, the study bases its analysis on an integrated perspective on the concept of risk
- advocating – for example, the work argues that the IRGC framework provides a useful guidance document for obtaining an inclusive, balanced, fair and effective risk governance process
- refuting – for example, the study argues that traditional probability-based risk management is not suitable for this case.

The research studies a concrete activity (petroleum operations in the Barents Sea area), relates it to a concept developed (the IRGC risk governance framework) and draws some conclusions using argumentation. It provides knowledge about the risk management and governance of this specific activity, and it provides input to how the concept works.

A hypothetical study of the antifragility concept

To demonstrate a traditional A type of research, we can think of a hypothetical study of pupils, with the aim of testing the hypothesis that 'An antifragile attitude leads to improved school performance'. The idea is to see whether loving some level of stress, risk and uncertainties actually has positive effects on school results. The research can be carried out in accordance with the

principles of statistical hypothesis testing – the standard scientific method – using a proper research design, for example, defining an experimental group and a control group. We omit the details, as the method is well known.

How to handle risk related to passive smoking

To study the health effects of passive smoking, the standard scientific method is commonly used. There is a huge body of literature on the topic (e.g. Proctor 2011), showing that passive smoking has some negative effects, and many governments have banned smoking in public places. However, there are different views on the seriousness of the problem and deciding how to handle the risk is not straightforward. Research can be conducted to guide the decision-makers (politicians).

The research can be of different types. One category is to perform a standard scientific method based on questionnaires aimed at revealing people's attitudes to the issue and their willingness and enthusiasm for levying restrictions on where smoking is permitted. An alternative is to use qualitative methods, for example based on interviews, to explore individuals' views, experiences, beliefs and/or motivations related to passive smoking. Such research methods are well-documented in the social science literature (e.g. Walliman 2011). They all integrate empirical studies with some theoretical analysis.

Another type of research is founded on economic theory and is also based on the combination of theory and empirical studies. Using cost-benefit type of studies, the aim is to reveal the value of potential measures (here, ban passive smoking) and obtain 'optimal' use of societal resources. In UK (2006), such a work is applied, and it is indicated that the decision to ban smoking in public places may represent a disproportionate response to a relatively minor health concern. We will return to this conclusion in the discussion in Section 3.2.3.

A comparison of risk regulation in Europe and the US

Considerable research has been conducted to investigate the extent to which Europe or the United States adopts a more precautionary position to the regulation of safety and health risks (Wiener and Rogers 2002, Hammitt et al. 2005, Löfstedt and Vogel 2001). This research compares the actual levels and trends in the regulations, using examples to support the conclusions. Some of the work is based on detailed analysis of a few non-random selected cases, whereas other work uses a quite comprehensive list of risks. The empirical analysis is built on theoretical frameworks for understanding, assessing, communicating and managing risk (the B type of knowledge). The observations and theoretical analysis are used to investigate the factors that

could explain some of the differences found, for example linked to political systems, risk perceptions, trade protectionism and legal systems.

Using risk analysis to describe climate risk and support relevant decision-making

We return to the climate change issue discussed in Section 1.1. Through a number of studies, the IPCC has characterized risk and uncertainties in relation to climate change. As risk analysis researchers, we can question the quality of the risk and uncertainty analysis on which the IPCC work is based, in particular the guidance note for lead authors of the fifth IPCC assessment report on consistent treatment of uncertainties (IPCC 2010). This is exactly what the research documented in Aven and Renn (2015) does. It compares the IPCC concepts and related justification with those of the risk analysis field as interpreted by the authors. The work points to strengths and weaknesses in the IPCC analysis. It is argued that the work carried out by the IPCC does not provide a theoretically and conceptually convincing basis for the treatment of risk and uncertainties. In addition, the research suggests improvements to the current IPCC concepts, to overcome the problems identified.

The research is related to type A as defined in Section 3.1, as it relates to a specific application – climate change – but also to type B, as the application builds strongly on the generic risk research.

Returning to the research features for conceptual analysis, as referred to in Section 3.2.1, this Aven and Renn (2015) IPCC research makes use of all these:

- identification – for example, the study identifies those principles that the IPCC recommends for use when characterizing uncertainties
- revision – for example, the work provides new interpretations for the type of probabilities used in the IPCC reports
- delineation – for example, the work does not include evaluation of specific models for analysing risk and uncertainties – only the fundamental concepts and principles
- summarization – for example, the study uses the IPCC (2010) document to summarize the IPCC way of dealing with uncertainties and risk
- differentiation – for example, the work differentiates between different types of probabilities
- integration – for example, the study bases its analysis on an integrated perspective on the concept of risk
- advocating – for example, the work argues that a modified perspective on risk and uncertainty has a stronger scientific basis than the current IPCC fundament
- refuting – for example, the study argues that the current IPCC approach to risk and uncertainties has severe weaknesses.

3.2.3 Discussion

The analysis in Section 3.2.2 demonstrates the importance of conceptual research in risk analysis. The core research method is conceptual, with varying degrees of empiricism supporting it. The present book is an example of this. It is a conceptual study with cases to illustrate and provide support for the argumentation provided. However, the main contribution to knowledge generation comes from conceptual thinking.

We see from the above discussion that there is a close link between the A and B types of knowledge generation. For example, when studying the IPCC approach to risk and uncertainty, the focus is on the application 'climate change', but the source for Aven and Renn's (2015) analysis is the generic B type of knowledge on the risk analysis concept. The example shows how the B knowledge can improve the A knowledge.

Reversed, the A knowledge can provide useful input for the B knowledge. For example, the studies concerning differences between Europe and the US related to the precautionary principle raised fundamental questions about the meaning and rationale of this principle. Generic research of type B is the result, as demonstrated in the discussion by Aven (2011a), Cox (2011) North (2011) and Vlek (2011). Knowledge production of type A is often in the form of statements characterizing 'the world', for example that a specific chemical is dangerous. The research provides evidence for this statement. Risk analysis supports the research by framing the problem and offering suitable concepts. The A type of research is driven by natural sciences, social sciences, psychology, etc., and a main challenge for the research (as discussed in Section 3.1.3) is to find a balance between confidence – there is a conclusion to be made (for example, that the chemical is dangerous) – and humility – there are uncertainties and risks involved: the conclusions can be wrong. Risk analysis research has an important role in clarifying how far this confidence can be stretched and how the humility should balance the confidence. Risk analysis provides substance to the concept of humility in relation to these sciences. The B type of risk analysis research represents the source for this input, but the actual implementation in relation to an application is an A type of risk analysis research.

An example illustrating this discussion is the UK (2006) report on passive smoking. It is indicated that the decision to ban smoking in public places may represent a disproportionate response to a relatively minor health concern, as mentioned in Section 3.2.2. Risk analysis research provides knowledge on how to think in relation to issues like this. It discusses the possible perspectives and arguments being used. As shown by Aven and Renn (2018), the UK (2006) report can be criticized for not really being in line with current risk management knowledge, as it adopts a narrow cost-benefit type of analysis; see Sections 7.3.2 and 7.5.2.

There are many ways of categorizing research, as discussed above. This is reflected in different ways of categorizing scientific papers. The following lists some typical categories used:

- Development of new methods and models
- Application of specific methods and models, with discussion
- Evaluation of specific methods and models
- Phenomenological studies (including empirical research)
- Review and discussion
- Others

Many journals have a main split between 'research papers' and 'perspective papers'. Both categories of papers are scientific, but only the first one is labelled research. This is unfortunate, as all the scientific papers are research papers. They produce scientific knowledge. Following the logic of science and research here adopted (refer to Fuchs 2005), see Section 2.1, research is specific work being carried out within the scientific system (the risk analysis discipline), for example work leading to some papers published in scientific journals.

3.2.4 Conclusions

Risk analysis research is based on the use of methods similar to those in other fields and sciences, for example statistics. To develop a concept (principle, theory, method, model), the main method used is conceptual. There will nearly always be an empirical basis, and examples will be used to motivate and illustrate the conceptual analysis, but the main research contribution is conceptual: a new, modified, evaluated or enhanced concept. The conceptual research and knowledge are used in applications, which are typically multidisciplinary and interdisciplinary. These risk analysis applications are based on the use of standard research methods, as we find them in natural sciences and social sciences. The traditional scientific method has a central place.

Research is about knowledge generation. Such knowledge generation is built on data, information, testing, theories, modelling and argumentation. It is essential, for the development of the risk analysis field and science, to acknowledge its dependence on and the importance of conceptual research. The argumentation for what is high-quality risk analysis and what is not represents a core element of the knowledge base of the risk analysis field and science. It is a common misconception that risk analysis is mainly founded on empirical studies of various phenomena. A broad spectrum of research methods is needed, as discussed and argued for above.

4 Fundamentals about the risk concept and how to describe risk

This chapter looks more closely into the risk concept, following up the overall ideas outlined in Section 3.1. First, Section 4.1 makes some overall reflections on what the concept of risk means, while Section 4.2 discusses how to describe or characterize risk. Then, Section 4.3 discusses some important features of the theory presented in Sections 4.1 and 4.2. Section 4.4 provides some conclusions.

4.1 THE RISK CONCEPT

Several attempts have been made to establish broadly accepted definitions of key terms related to concepts fundamental for the risk field (see e.g. Thompson et al. 2005). A scientific field or discipline needs to stand solidly on well-defined and universally understood terms and concepts. Nonetheless, experience has shown that to agree on one unified set of definitions is not realistic. This was the point of departure for a thinking process conducted recently by an expert committee of the Society for Risk Analysis (SRA), which resulted in a new glossary for SRA (SRA 2015a). The glossary is founded on the idea that it is still possible to establish authoritative definitions, the key being to allow for different definitions on fundamental concepts and to make a distinction between overall qualitative definitions and their associated measurements.

Allowing for different definitions does not mean that all suggestions that can be found in the literature are included in the glossary: the definitions included have to meet some basic criteria, having a rationale, and being logical, well-defined, understandable, precise, etc.

Here is the risk definition text from SRA (2015a):

> We consider a future activity (interpreted in a wide sense to also cover, for example, natural phenomena), for example the operation of a system, and define risk in relation to the consequences of this activity with respect to something that humans value. The consequences are often seen in relation to some reference values (planned values, objectives, etc.), and the focus is normally on negative, undesirable consequences. There is always at least one outcome that is considered as negative or undesirable. In a project, the issue of interest could be risk related to not meeting the defined cost target. The consequences C are then to be defined as the deviation between the target and the actual cost, and U relates to uncertainty about this deviation.
>
> Overall qualitative definitions of risk:
>
> a) the possibility of an unfortunate occurrence.
> b) the potential for realization of unwanted, negative consequences of an event
> c) exposure to a proposition (e.g. the occurrence of a loss) of which one is uncertain
> d) the consequences of the activity and associated uncertainties
> e) uncertainty about and severity of the consequences of an activity with respect to something that humans value
> f) the occurrences of some specified consequences of the activity and associated uncertainties
> g) the deviation from a reference value and associated uncertainties
>
> These definitions express basically the same idea, adding the uncertainty dimension to events and consequences.
>
> (SRA 2015a)

Thus, the risk concept has two main features – values or consequences C in relation to something that humans value, and uncertainty (possibility, potential) U: we do not know what C will be. Different ways of conceptualizing these two ideas are presented; see a–g. In the present book, they are simply referred to as the (C,U) representation of risk. Often the consequences explicitly refer to events A that can occur, leading to some effects. To highlight A, we write risk as (A,C,U). Thus, we use the term 'consequences' for all effects of the activity considered and the effects given the occurrence of A.

As an example, illustrating the concept of risk, think about the activity as driving a car at a particular point in time from place v to w. The consequences of the activity could be that the trip is successful or accident events (A) could occur, leading to injuries or fatalities (C). Before the trip is made,

we do not know what the consequences would be. There are uncertainties and, hence, risks: for the driver and his/her passengers, and possibly for other people exposed to the car.

A related activity is all car driving in a country in one year, where the consequences are focused on the number of fatalities (C). This number is unknown at the beginning of the year; there are uncertainties, there is risk present. Based on records from earlier years, we are able to provide informative descriptions of the uncertainties and risk, but then we are into the topic of the next section.

4.2 HOW TO DESCRIBE OR CHARACTERIZE RISK

To describe or measure risk – to make judgements about how large or small the risk is – different approaches and methods are used. SRA (2015a) provides some examples of "risk metrics/descriptions":

1. The combination of probability and magnitude/severity of consequences
2. The triplet (s_i, p_i, c_i), where s_i is the *i*th scenario, p_i is the probability of that scenario, and c_i is the consequence of the ith scenario, i = 1,2, . . . N
3. The triplet (C',Q,K), where C' is some specified consequences, Q a measure of uncertainty associated with C' (typically probability) and K the background knowledge that supports C' and Q (which includes a judgement of the strength of this knowledge)
4. Expected consequences (damage, loss), for example computed by:
    i. Expected number of fatalities in a specific period of time or the expected number of fatalities per unit of exposure time
    ii. The product of the probability of the hazard occurring and the probability that the relevant object is exposed given the hazard, and the expected damage given that the hazard occurs and the object is exposed to it (the last term is a vulnerability metric)
    iii. Expected disutility
5. A possibility distribution for the damage (for example a triangular possibility distribution)

The suitability of these metrics/descriptions depends on the situation. None of these examples can be viewed as risk itself, and the appropriateness of the metric/description can always be questioned. For example,

> the expected consequences can be informative for large populations and individual risk, but not otherwise. For a specific decision situation, a selected set of metrics have to be determined meeting the need for decision support.
>
> (SRA 2015a)

To illustrate the thinking, consider the personnel risk related to potential accidents on an offshore installation. Then, if risk is defined according to d, in line with the recommendations in for example PSA-N (2018a) and Aven et al. (2014), risk has two dimensions: the consequences of the operation covering events A, such as gas leakages and blowouts, and their effects C on human lives and health, as well as uncertainty U (we do not know now which events will occur and what the effects will be): we face risk. The risk is referred to as (A,C,U). To describe the risk, as we do in the risk assessment, we are in general terms led to the triplet (C',Q,K), as defined above. We may, for example, choose to focus on the number of fatalities, and then C' equals

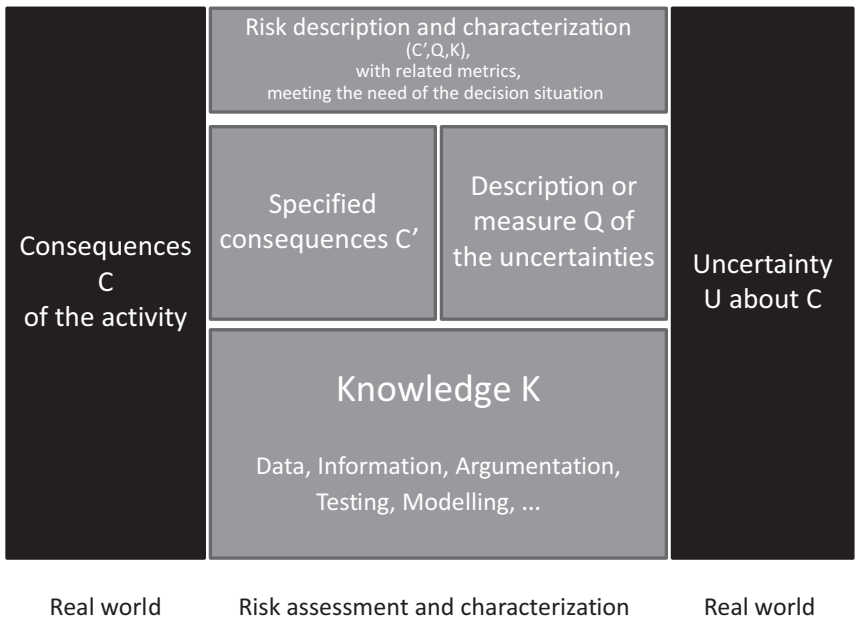


FIGURE 4.1 The risk of an activity of the real world captures C and U, the actual consequences of the activity and the associated uncertainties (what will C be?). In the risk assessment, C is specified as C', for example as the number of fatalities, and using a description of uncertainty Q (for example, probability and judgements of the strength of knowledge supporting the probabilities). K is the knowledge that Q is based on (figure based on Aven 2017b).

this number. It is unknown at the time of the analysis, and we use a measure (which is to be understood in a broad way) to express the uncertainty. Probability is the most common tool, but other tools also exist; see Section 4.2.2. In general, the present book recommends using probability (or probability intervals), together with judgements of the strength of knowledge supporting these probabilities; see Section 4.2.2. In the following, we will often talk about descriptions and characterizations of the uncertainties instead of measurement. Aven (2012a) provides a comprehensive overview of different categories of risk definitions, having also a historical and development trend perspective. It can be viewed as a foundation for the SRA (2015a) Glossary.

Figure 4.1 illustrates the concept of risk and its description, in its most generic form, in line with these perspectives.

The above framework for understanding and describing risk can be extended in many ways, for example by including 'barriers' and 'risk sources'.

- Barriers: Barriers, for example, protection measures to reduce the effects of radiation or a warning system when radiation is increasing above a threshold level, are introduced to avoid events occurring and to reduce the consequences of the events if they should in fact occur. The occurrences of the events and related consequences depend on the performance of these barriers.
- Risk sources and risk influencing factors: A risk source RS is an element (action, activity, component, system, event . . .), which alone or in combination has the potential to give rise to an event (A) with a consequence (C) related to the values of concern. Think about a human being exposed to radiation from uranium in soil and rock. The uranium can be considered a risk source RS, as can the soil and rock. This exposure may lead to cancer (A) and affect the health of the person (effect or consequences C). We are led to a trichotomy: the risk sources RS (uranium, soil and rock), the associated event A (cancer) and the consequences C (health effects).

  Note that a risk source can be an event, like failure in a system. Also, the event A can be considered a risk source. These concepts are relative, in the sense that they can be labelled both risk source (RS) or event (A), depending on the conditions we would like to highlight. In a simplified set-up, we use only the events A.

  We also use the term 'risk influencing factor' to have basically the same meaning as risk source: an aspect or condition that affects or influences risk.

  To illustrate these concepts, consider a company which is to study the risk related to climate change. For the company, the main focus is on its financial metrics, and changes in the environment due to climate change are to be considered a risk influencing factor (risk source) or an event.

Reference values are specified for the consequences, and risk is related to deviations from these and associated uncertainties.

Next, consider the climate risk from a planet perspective. An effect can, for example, be defined in relation to the increase in the global average temperature relative to the pre-industrial levels. There is risk related to this effect: it could be 2°C, lower or higher. Technology development and political decisions are to be viewed as risk influencing factors (risk sources).

- **Threat, hazard and opportunity:** In the above trichotomy, a threat can be viewed as the event A. In line with the SRA (2015a) Glossary, we use the term 'threat' in a broad sense, in the same way as the term 'risk source'. Threat is also commonly used, in relation to security, as an attack, as a stated or inferred intention to initiate an attack with the intention to inflict harm, fear, pain or misery (SRA 2015a). A hazard is a risk source or event where the potential consequences relate to harm, i.e. physical or psychological injury or damage, and normally restricted to safety applications. The judgement is that it is likely that the risk source or event leads to negative effects. An opportunity is a risk source or event, which has the potential – it is judged likely – to give rise to some specified desirable consequences.
- **Vulnerability:** As mentioned above, it is common to write (A,C,U), instead of (C,U), and we can similarly use the notation (A', C',Q,K) in the risk description to highlight the events – the threats and hazards preceding the effects. Introducing the events, we can think about the associated C and C' as conditional effects or consequences given the occurrence of this event.

  This leads us to a terminology where risk is seen as

  (Threat, uncertainties) and vulnerability or, using symbols:
  Risk = (A,U) + (C,U|A),

where vulnerability is the effect or consequences conditional on the occurrence of the event A. Here, | A' means 'given the occurrence of A'. The symbol '+' is here not to be interpreted as a sum, as in mathematics, but as a symbol for combining the two elements. Similarly, we can write

Risk description = (A',Q,K) + (C',Q,K|A'),

which expresses that risk is described by the combination of the uncertainty characterization of the threat and the vulnerability given the occurrence of the event A'. See Section 7.4 for some reflections on (C,U|A) and the concept of resilience.

- **Safety and security:** We define safe as being without unacceptable risk, and safety is interpreted in the same way (e.g. when saying that safety is achieved). We also talk about safety as the antonym of risk (the safety level is linked to the risk level; a high level of safety means a low risk level and vice versa). Analogously, we define secure as being without unacceptable risk when restricting the concept of risk to intentional unwanted acts by intelligent actors. Security is interpreted in the same way as secure (e.g. when saying that security is achieved) and as the antonym of risk when restricting the concept of risk to intentional unwanted acts by intelligent actors (the security level is linked to the risk level; a high security level means a low risk level and vice versa). Through these definitions, the key concept is risk, as safe and secure are defined on the basis of this term.

  In security contexts, it is common to refer to the triplet: value, threat and vulnerability (Amundrud et al. 2017). This perspective is included in the above general framework. The values are identified, and the consequences C of the events A and risk sources RS relate to these values. The threats T are defined as either events A or RS, and the uncertainty U associated with the occurrence of the threats is addressed. Given the occurrence of a threat, we look into the consequences, together with the associated uncertainties, which are referred to as the vulnerability. These are the fundamental concepts defining risk; next, we need to describe the risk. Then we specify threats T' (risk sources RS', events A') and consequences C' and use a measure of uncertainty Q, which is based on some background knowledge K, leading to a description of risk equal to (T', C', Q, K). The uncertainty measure Q could be a mixture of (interval) probability, assessments of intentions and capabilities, as well as judgements of the strength of knowledge supporting the other assessments; refer to Amundrud and Aven (2015), Amundrud et al. (2017) and Askeland et al. (2017).

The way we understand and describe risk strongly influences the way risk is analysed and, hence, it may have serious implications for risk management and decision-making. There is no reason why some of the current perspectives should not be wiped out, as they are simply misguiding the decision-maker in many cases. The best example is the use of expected loss as a general concept of risk. This approach fails to reflect important aspects of risk: the potential for large or extreme outcomes, as well as the strength of knowledge supporting the judgements made. The uncertainty-founded risk perspectives as defined above indicate that we should also include the pure probability-based perspectives, as the uncertainties are not sufficiently revealed for these perspectives (see discussion in the following and also Aven 2012a).

By starting from the overall qualitative risk concept, we acknowledge that any tool we use needs to be treated as a tool. It always has limitations, and these must be given due attention. Through this distinction, we will more easily look for what is missing between the overall concept and the tool. Without a proper framework clarifying the difference between the overall risk concept and how it is being measured, it is difficult to know what to look for and make improvements in these tools.

A generic risk concept and related characterizations exist, relevant for all applications: The risk concept is addressed in all fields, whether finance, safety engineering, health, transportation, security or supply chain management (Althaus 2005). Its meaning is a topic of concern in all areas. Some areas seem to have found the answer a long time ago, for instance the nuclear industry, which has been founded on the Kaplan and Garrick (1981) definition (the triplet scenarios, consequences and probabilities) for more than three decades; others acknowledge the need for further developments, such as in the supply chain field (Heckmann et al. 2015). Heckmann et al. (2015) point to the lack of clarity in understanding what the supply chain risk concept means and search for solutions. A new definition is suggested: "Supply chain risk is the potential loss for a supply chain in terms of its target values of efficiency and effectiveness evoked by uncertain developments of supply chain characteristics whose changes were caused by the occurrence of triggering-events". The authors highlight that "The real challenge in the field of supply chain risk management is still the quantification and modelling of supply chain risk. To this date, supply chain risk management suffers from the lack of a clear and adequate quantitative measure for supply chain risk that respects the characteristics of modern supply chains" (Heckmann et al. 2015).

We see a structure resembling the structure of the SRA Glossary, with a broad qualitative concept and metrics describing the risk. The supply chain risk is just an example to illustrate the wide set of applications that relate to risk. Although all areas have special needs, they all face risk as framed in the set-up of the first paragraph of the SRA (2015a) text in Section 4.1. There is no need to invent the wheel for every new type of application.

To illustrate the many types of issues associated with the challenge of establishing suitable risk descriptions and metrics, an example from finance, business and operational research will be provided. It is beyond the scope of the present book to provide a comprehensive all-inclusive overview of contributions of this type.

- **Value-at-Risk (VaR):** In finance, business and operational research, there is considerable work related to risk metrics, covering both moment-based and quantile-based metrics. The former category covers, for

example, expected loss functions and expected square loss, and the latter category, Value-at-Risk (VaR), and Conditional Value-at-Risk (CvaR); see, for example, Natarajan et al. (2009) and Aven (2010c). Research is conducted to analyse their properties and explore how successful they are in providing informative risk descriptions in a decision-making context, under various conditions, for example for a portfolio of projects or securities, and varying degrees of uncertainties related to the parameters of the probability models; see, for example, Natarajan et al. (2009), Shapiro (2013), Brandtner (2013) and Mitra et al. (2015). As these references show, the works often have a rigorous mathematical and probabilistic basis, with strong pillars taken from economic theory such as the expected utility theory. A main problem with the VaR index is that it does not reflect well the potential for extreme outcomes: Two probability distributions could have the same VaR but completely different tails (Aven 2010c, p. 37).

The specific ways risk can be characterized are many and, in the following section, alternative approaches and methods will be presented and discussed. The characterizations need to address both C and U; we need to specify C and find ways of representing or expressing the uncertainties. To characterize risk, a risk assessment is conducted. The characterizations should meet the needs of both the risk assessment and the decision-making the assessment is to support. There are, however, some fundamental ideas and principles to be followed that are generic and applicable to all types of situations. These we highlight in the present book. First, we address the consequences C (Section 4.2.1). Then, we will look at the uncertainties U (Section 4.2.2). In Section 4.2.3, these elements are integrated, resulting in a full risk characterization. Section 4.2.4 presents and discusses some examples.

4.2.1 Describing the consequences C of the activity considered

In the risk assessment, we need to clarify which aspects of the consequences we would like to address. This relates to two main dimensions: i) the values we are concerned about (lives, environment, assets, etc.) and ii) the level of scenario development elements (risk sources, events, barrier performance, outcomes). Examples of these elements related to lives for a petroleum installation could be maintenance, occurrence of a leakage, the performance of a lifeboat, and the number of fatalities, respectively. A potential risk factor (source) is maintenance, giving rise to a process leakage, which in its turn could result in loss of lives, depending on the presence and performance of various barriers, for example lifeboats. The consequences C cover all these

scenario development elements, but often the risk characterization focuses only on the outcomes: here, the number of fatalities. However, in other cases, all these elements are highlighted; for example, this is the case when the authorities present the risk level of the Norwegian petroleum activities (PSA-N 2018b). The number of leakages could be more informative than the number of fatalities in many cases, as the latter number is often zero for safe systems.

Let C' denote the consequences specified in the risk assessment, capturing the quantities of interest. Similar to C, some components of the specified consequences C' can express deviations relative to some specified goals or targets.

Models

The scenario development can be just a listing of the elements, or it can be based on modelling, using tools such as fault trees, event trees and Bayesian networks. The modelling means simplified representations of the relationships between the various elements. Let C'_1 denote the number of fatalities in the future period studied, and let g(X) express the model used to compute C'_1, i.e. $C'_1 = g(X)$, where X is a vector of elements. If C_1 denotes the actual number of fatalities, we can identify a difference, $e = g(X) - C_1$, which is referred to as model (output) error. See Section 5.3 for further details.

Observables and probability models

What characterizes the above scenario development elements is that they are observable quantities, in the sense that if the activity is realized we can observe the number of fatalities, the occurrence or not of a leakage, etc. In risk analysis, we also use unobservable quantities, typically defined as parameters of probability models. A probability model is a model of a phenomenon in the real world, represented by means of frequentist probabilities, as explained in Section 3.1.1. A frequentist probability of an event A is interpreted as the fraction of times A occurs if we could infinitely repeat the situation considered under similar conditions.

For example, to model the occurrences of gas leakages, we may introduce a Poisson distribution with parameter (expected value) λ. It is well known from probability theory that, if we assume the same probability of a gas leakage occurrence for all small intervals in a specified period, and the intervals are independent, the probability distribution of the number of events can be well approximated by the Poisson distribution; see below.

Now, consider again the activity generating the consequences C. We may ask: where are the probability models and their parameters? The answer is: they are not there, as C is the actual consequences, and probability models do not exist in the real world, they are constructions made by us to study

the real world. Then we can raise the same question for the specified consequences C': where are the probability models and their parameters? Now we can find them. When probability models are introduced, we obtain parameters and quantities of interest that are expressed through frequentist probabilities P_f or related expected values E_f. For example, if a probability model is introduced for the number of fatalities, a frequentist probability p of a fatal accident next year can be defined. The parameter λ of the Poisson model represents the expected number of gas leakages and is interpreted as the average number of leakages, when considering an infinite number of similar situations to the one studied.

Using analysis tools such as fault trees, event trees and Bayesian networks, models are developed linking low-level probabilistic parameters (linked to leakages and barriers) with the high-level probabilistic parameters (linked to the number of fatalities).

Key quantities of interest: observables or probabilistic parameters?

Risk assessments and risk characterizations can be conducted with and without the use of models and particularly probability models. When probability models can be justified and are introduced, they should be seen as a tool for gaining insights and supporting the analysis and uncertainty judgements to be made concerning the observable components of C', as will be discussed in the coming section. The analysts always need to carefully judge: what really are the key quantities of interest – the observables or the probabilistic parameters?

For example, when studying the risk related to the occurrence of a disease in a huge population, a frequentist probability would accurately approximate the fraction of persons having this disease in this population, and a focus of the analysis on this frequentist probability would normally be preferred. However, if the aim of the study is to address the risk related to a specific person with his/her specific characteristics, such a macro perspective would not be sufficient. It could provide useful background knowledge for the analysis, but the observables related to the person (he or she contracting the disease or not) would need to be the main focus.

The case of rare events

Consider the task of analysing rare events with extreme consequences. To this end, a probabilistic framework is often used, founded on the use of probability models. Reference is made to concepts like heavy and fat distribution tales. However, we seldom see that this framework is justified or questioned. Is it in fact suitable for studying extreme event phenomena?

A probability model is established based on reasoning, as for the binomial or Poisson distributions or by estimations based on observations. Both approaches introduce uncertainties, as explained in the following.

If the probability model is based on reasoning, there will be a set of assumptions that the modelling is founded on. For example, in the homogeneous Poisson case, the probability of an event occurring in a small interval $(t, t+h)$ is approximately equal to λh, for a fixed number λ, independent of the history up to t. Verifying such assumptions is, however, in general difficult, as there may be little relevant data that can be used to check them, particularly in the case of rare events. Estimations and model validation using observations are applicable when huge data sets are available but not when studying extreme events. The consequence is that the analysis simply needs to presume the existence of the model and the results interpreted as conditional on these assumptions. Thus, care has to be shown in making conclusions based on the analysis, as the assumptions could cover or conceal important aspects of uncertainties and risks.

Introducing a probability model needs to serve a purpose. The common argument used is that it allows for statistical inference, to apply the strong machineries of statistics and Bayesian analysis, updating our knowledge when new information becomes available (Lindley 2000). For situations where the degree of variation is the key aspect or quantity of interest, such models surely have a role to play, but, in cases of extreme events, variation is not really the interesting concept, as there is no natural family of situations that these events belong to. Take major nuclear accidents. For the industry, historical data are informative on what has happened and how frequently. But will the development and use of a probability model for representing the variation in the occurrences of such accidents lead to new and important insights? To provide an answer to this question, let us review the potential purposes for developing such a model:

a) To predict the occurrence of coming events
b) To show trends
c) To present 'true' risk levels
d) To facilitate continuous updating of information about the risk levels

Clearly, the use of such models does not allow for accurate prediction of occurrences, as the data are so few and the future is not necessarily reflected well by these data. Hence, a) is not valid. We must conclude the same when it comes to b) for the same reasons: meaningful trends cannot be established when the data basis is weak. Consider the risk quantity defined by the frequentist probability that a major nuclear accident occurs in a country in the next year. As discussed above, it is challenging to give this probability an interpretation, as it requires the definition of an infinite population of

similar situations to the one studied. Anyway, it is unknown and needs to be estimated. With a weak database, this estimate could deviate strongly from the 'true' frequentist probability. Hence, c) is also problematic. Probability modelling is an essential pillar for using Bayesian analysis to systematically update the knowledge when new information becomes available. However, the modelling needs to be justified for the results to be useful. As discussed above, the problem is that it is often difficult to establish in a meaningful way an infinite population of similar situations or units. There is always a need to formulate a hypothesis, as knowledge generation is built on theory (Lewis 1929, Bergman 2009, Deming 2000, p. 102), but, in cases of rare events, broader frameworks than probabilistic modelling are required. Judgements of risk for such events cannot be based on macro statistical data and analysis. More in-depth analysis of risk sources, threats, barriers, consequences is needed, in other words more in-depth risk assessments.

Propensity interpretation of probability

Instead of considering probability models as a tool for modelling variation, it is also common to think of the model as a representation of characteristics of the activity or system, using the 'propensity' interpretation of probability. For the propensity interpretation, suppose we have a special coin; its characteristics (centre of mass, weight, shape, etc.) are such that, when tossing the coin over and over again, the head fraction will reach a number, the head propensity of the coin. However, accepting the framework of the frequentist probability, i.e. that an infinite sequence of similar situations can be generated, is practically the same as accepting the idea of the propensity interpretation, as it basically states that such a framework exists (Aven and Reniers 2013). The propensity can be seen as a repeatable experimental set-up, which produces outcomes with a limiting relative frequency, which equals the frequentist probability (SEP 2011).

4.2.2 Describing the uncertainties U

The quantities C' introduced in the previous section are unknown and thus subject to uncertainties; they are either observables or parameters of probability models. The challenge next is to represent or express these uncertainties. Basically, for doing this, there are two ways of thinking:

i) Seek to obtain a characterization of the uncertainties that to the extent possible are objective or intersubjective, reflecting the evidence available.
ii) Provide a subjective characterization of the uncertainties by the risk analysts, reflecting their knowledge and judgements, often on the basis of input from other experts.

A simple example will illustrate the differences between these two perspectives. A person refers to a special coin, with unknown frequentist probabilities for head and tail. This person does not see the coin. Let r be the frequentist probability of head. The assessor has no knowledge about r, and the question is how to represent or express the uncertainties about r.

A common approach is to assume a uniform distribution over r. However, by introducing such a distribution, the assessor expresses, for example, that the probability of r being in the interval [0, ½] is the same as r being in the interval [1/2, 1]. It seems that the approach is of the ii type. But where did the probability judgements come from? They are to reflect the knowledge or judgement of the analyst, but, for the problem we defined, we excluded this type of insights or judgements. Hence, something has been added which was not originally available. The use of probability distribution forces the analyst to express his/her degree of belief for different values of r. The information value of this distribution may be more or less strong, as the basis for it may be more or less strong. Thus, using such probabilities alone to characterize the uncertainties is problematic, if not also reflecting in some way the knowledge on which the probabilities are based. See related discussion by Dubois (2010) and Aven (2010b).

The alternative is to apply i, which forces the analyst to simply express that r is in the interval [0,1]. Based on the available knowledge, he/she cannot say anything more. We see that such an approach is rather extreme in the other direction, compared to ii; here, we are led to a very wide interval, saying really nothing. The presentation is more objective, but the information value for the decision-maker is strongly reduced. More information is clearly needed to make this approach useful. Suppose that the experts express that ½ is the most likely value of r. Then we are led to interval (imprecise) probabilities, expressing, for example, that $0 \leq P(r \leq 0.25) \leq 0.5$, $0 \leq P(r \leq ½) \leq 1.0$ and $0.5 \leq P(r \leq 0.75) \leq 1.0$ (see Aven et al. 2014, p. 47). The analyst is not willing to be more precise than this, given the information and knowledge available. However, in this case, we also need to address the knowledge and strength of knowledge supporting these interval probabilities. The basis for the expert judgement of $r = ½$ could be poor or strong, but this is not reflected in the probabilities assigned. The transformation process from the evidence to the probabilities is here 'objective', but of course the knowledge *per se* is not.

Logical probabilities

The idea of the logical probability is that it expresses the objective degree of logical support that some evidence gives to the event (a hypothesis being true). It is believed that there is a direct link between evidence and the probability. The idea of such probabilities is however problematic, as Dennis Lindley writes:

> Some people have put forward the argument that the only reason two persons differ in their beliefs about an event is that they have different knowledge bases, and that if these bases were shared, the two people would have the same beliefs, and therefore the same probability. This would remove the personal element from probability and it would logically follow that with knowledge base K for an uncertain event E, all would have the same uncertainty, and therefore the same probability P(E|K), called a logical probability. We do not share this view, partly because it is very difficult to say what is meant by two knowledge bases being the same. In particular it has proved impossible to say what is meant by being ignorant of an event, or having an empty knowledge base, and although special cases can be covered, the general concept of ignorance has not yielded to analysis.
>
> (Lindley 2006, p. 44)

The concept of logical probability has never received a satisfactory interpretation; see for example Cooke (2004) and Aven (2015c). Using logical probabilities, we are not able to interpret what a probability of say 0.1 means, compared to 0.2. It should therefore be rejected.

The measure or description Q

In general terms, the challenge is to represent or express our uncertainties about C'. 'Our' refers here to the analyst or any other person who conducts the judgements. Let Q be such a representation or expression of uncertainty. Basically, there are two ways of thinking in specifying Q, giving it an interpretation and determining its value in a concrete case, in line with i and ii.

The description Q represents or expresses epistemic uncertainties about C', as C' is not known – the result of insufficient knowledge. Epistemic uncertainty can be reduced if additional information and knowledge can be acquired.

Subjective probabilities – the search for a proper interpretation

Approach ii is commonly implemented using subjective probabilities; hence Q = P. The scientific literature on subjective probabilities is, however, rather chaotic, in the sense that the earlier and historical interpretations of this probability are still referred to, despite the fact that these are based on unfortunate mixtures of uncertainty judgements and value judgements (Aven and Reniers 2013). If the science of uncertainty analysis offers this type of interpretation, it is not surprising at all that it is not very much used in practice. Consider the following example. We are to assign a subjective probability for the event A to occur or a statement A to be true, for example that most of the global warming is the result of human activity (refer to Section 1.1).

A probability of 0.95 is assigned. Following common schools of thought in uncertainty analysis, this probability P(A) is to be understood as expressing that 0.95 is "the price at which the person assigning the probability is neutral between buying and selling a ticket that is worth one unit of payment if the event occurs (the statement is true), and worthless if not" (see e.g. SEP 2011, Aven and Reniers 2013). Such an interpretation cannot and should not be used for expressing uncertainty, as it reflects the assigner's attitude to money; see the discussions in Lindley (2006), Cooke (1986) and Aven and Reniers (2013). If we are to be informed by the uncertainty judgements, we would not like them to be influenced by these experts' attitude to dollars. It is absolutely irrelevant for the uncertainty judgement.

Many other perspectives on subjective probabilities exist, and one often referred to is the Savage interpretation, based on the basis of *preferences* between acts; see Bedford and Cooke (2001). The idea is that the subjective probability can be determined based on observations of choices in preferences. However, as these preferences relate to money or other value attributes, the same problem occurs as above; we do not produce pure uncertainty judgements but a mixture of uncertainty and value judgements, which makes, for example, a statement like P=0.95 in the climate change case impossible to meaningfully interpret.

How to interpret a subjective probability and subjective imprecise probabilities

Fortunately, a theory and meaningful operational procedures exist that can be used to specify subjective probabilities as a pure measure of uncertainty; see Lindley (1970, 1985, 2000, 2006). A subjective probability of 0.95 is here interpreted as expressing that the assigner has the same uncertainty and degree of belief in the event A occurring (or the statement A to be true) as randomly drawing a red ball out of an urn, which comprises 100 balls, of which 95 are red; refer to Section 3.1. This way of understanding a probability was referred to by Kaplan and Garrick (1981) in their celebrated paper about risk quantification, but there are few examples of researchers and probabilists adopting this way of interpreting probability (Aven and Reniers 2013). This is unfortunate, as it provides a simple, elegant and easily understandable basis and theory for subjective probability. A subjective probability is also referred to as a knowledge-based or judgemental probability. In the following, we will frequently refer to knowledge-based probability when interpreting probability using this type of urn reference.

A knowledge-based probability is personal, depending on the assigner and the knowledge supporting the assignment. This fact has led scholars to look for alternative approaches for representing or expressing the uncertainties, as the probability number produced in many cases has a weak basis.

The probability assigned seems rather arbitrary and too dependent on the assigner. That scientific knowledge generation requires more objective results is a common way of reasoning. It motivates the alternative approach i, an objective representation/transformation of the knowledge K available, to Q. There are different ways of obtaining such a representation/transformation, but the most common one is the use of probability intervals – also referred to as imprecise probabilities. In the climate change case, an interval probability of [0.95,1] is specified. This does not mean that the probability is uncertain, as there is no reference to a 'true' probability; it simply means that the assigner is not willing to be more precise, given the knowledge available. Hence, the assigner expresses that his/her degree of belief in the event occurring or the statement being true is equal to or higher than an urn chance of 0.95. His/her uncertainty or degree of belief is comparable with randomly drawing a red ball out of an urn comprising 100 balls, of which 95 or more are red. Betting-type interpretations are also commonly used for interpreting interval probabilities, but they should be rejected for the same reasons as given above for the subjective probabilities.

Studying the literature related to the challenge of i, one soon realizes that this is indeed a rather confusing area of analysis and research. There are different theories: possibility theory, evidence theory, fuzzy set theory, etc. with fancy mathematics, but the essential points motivating these theories are often difficult to reveal. Interpretations of basic concepts are often missing.

The issue of objectivity in relation to imprecise probabilities

The above analysis is an attempt to clarify some of the issues discussed. The aim of the alternative approaches is to obtain a more objective representation of uncertainty given the knowledge available. This is often misinterpreted as saying that the representation is objective. Clearly, the objectivity here just refers to the transformation from K to Q. Using P alone, it is acknowledged that there is a leap from K to Q, which is subjective. With a probability interval (imprecise probability), this leap is reduced or eliminated. The knowledge K can, however, be strongly subjective, more or less strong and even erroneous, for example if it represents the judgement by one expert.

In practice, it can be attractive to use both i and ii. The latter approach ensures that the analysts' and experts' judgements are reported and communicated, whereas the former approach restricts its results to a representation of documented knowledge.

The strength of the knowledge K

Any judgement of uncertainty is based on some knowledge K, and this knowledge can be more or less strong. How should this be reported?

In the IPCC work, a qualitative measure of confidence is used with five qualifiers: very low, low, medium, high and very high, reflecting strength of evidence and degree of agreement (IPCC 2010, 2014a). The strength of evidence is based on judgements of "the type, amount, quality, and consistency of evidence (e.g., mechanistic understanding, theory, data, models, expert judgment)" (IPCC 2014a). Consider the following statements from the IPCC (2014a):

> ocean acidification will increase for centuries if CO2 emissions continue, and will strongly affect marine ecosystems (with high confidence). IPCC (2014a, p. 16) (4.1)
>
> The threshold for the loss of the Greenland ice sheet over a millennium or more, and an associated sea level rise of up to 7 m, is greater than about 1°C (low confidence) but less than about 4°C (medium confidence) of global warming with respect to pre-industrial temperatures. (IPCC 2014a, p. 16) (4.2)

There are no explicit uncertainty judgements of the form Q used in these cases. But, could not the first example (4.1) be interpreted as expressing that "Ocean acidification will increase for centuries if CO2 emissions continue, and will strongly affect marine ecosystems" is true with very high probability? Yes, such an interpretation is reasonable, but, according to the IPCC (2010, p. 3), "Confidence is not to be interpreted probabilistically". What the IPCC says is that (4.1) expresses that the statement of interest is true with high confidence. Knowledge-based probabilities are not used to reflect uncertainties.

Let us look into statement (4.2). For example, if "is greater than about 1°C" with low confidence, what does this statement really express? Is there a reason to believe that the statement is true? Without any reference to a knowledge-based probability, it is impossible to know. According to Aven and Renn (2015), the IPCC framework lacks a proper uncertainty and risk analysis foundation, as the link between the strength of knowledge (confidence measure) and Q is not clarified.

One possible interpretation of the IPCC framework is that it builds on imprecise probabilities of the form [0,1], i.e. a complete lack of willingness to specify any probability interval beyond the trivial one [0,1], in addition to the strength of knowledge (confidence) judgements. The approach recommended in this book is more general and allows the analyst to express the uncertainties using either exact or imprecise knowledge-based probabilities. Depending on the situation considered and in particular the knowledge strength, different choices of imprecision intervals may be applied, leading

to the combined pair of knowledge-based probabilities (exact or imprecise) and supporting strength of knowledge judgements.

The IPCC concept of confidence is based on the two dimensions, evidence and agreements. The latter criterion needs to be implemented with care; if agreement is among experts within the same 'school of thought', its contribution to confidence is much less than if the agreement is built on experts representing different areas, disciplines, etc. (Miller 2013, Aven and Ylonen 2018).

Yet, we find this criterion in most systems for assessing strength of knowledge and confidence; see, for example, Flage and Aven (2009) and Aven and Flage (2018), who establish a qualitative strength of knowledge scheme based on judgements of issues such as:

- The reasonability of the assumptions made
- The amount and relevancy of data/information
- The degree of agreement among experts
- The degree to which the phenomena involved are understood and accurate models exist
- The degree to which the knowledge K has been thoroughly examined (for example with respect to unknown knowns; i.e. others have the knowledge but not the analysis group).

For some concrete examples of scoring systems based on such issues, see Aven (2017c) and Section 5.5.2.

As another example to explain the importance of the background knowledge, think about criminal law. Here, the quantity of interest is X, defined as 1 or 0, depending on whether the defendant did or did not commit the crime. The guilt G (i.e. X=1) is uncertain and can be described by a probability. Data, in the form of evidence K, are produced and the probability updated to P(G|K); see Lindley (2000) for how this updating can be conducted using the Bayesian formula and approach. The point to be made here is that it is not enough to just report the probability number without also addressing the strength of the evidence supporting the probability. Clearly, if this strength is weak, the probability judgement cannot be given much weight. The probability judgements will provide useful information for the decision-makers, but, equally, if not more, important is the evidence and its strength.

Basic probability theory is illustrative for showing why the knowledge dimension needs to be included in the risk characterizations: when using probability models with unknown parameters, we can use the law of total probability to obtain so-called predictive distributions of observables.

Consider again the Poisson example. If we assign a density $f(\lambda)$ to the unknown parameter λ, we obtain the unconditional predictive distribution of the number of events X_1, by the law of total probability:

$$P(X_1 = x) = \int P(X_1 = x|\lambda)f(\lambda)d\lambda = \int p(x|\lambda)f(\lambda)d\lambda, \quad (4.3)$$

where $p(x|\lambda)$ is the Poisson distribution function. At first glance, one may think that it is also possible to 'integrate out' the knowledge K from the equation and limit the uncertainty characterizations to probability. However, this is not possible. A knowledge-based probability is always conditional on some knowledge. Even in the case when the parameter λ is 'integrated out' in Formula (4.3), we need to think about the knowledge supporting f when evaluating $P(X_1 = x \mid K)$, as well as the knowledge supporting the Poisson model $p(x|\lambda)$.

For a related qualitative scheme for assessing the knowledge strength, see the so-called NUSAP system (NUSAP: Numeral, Unit, Spread, Assessment and Pedigree) (Funtowicz and Ravetz 1990, 1993, Kloprogge et al. 2005, 2011, Laes et al. 2011, van der Sluijs et al. 2005a, 2005b, Berner and Flage 2016b). In this system, agreement is also identified as a criterion, in fact among both peers and stakeholders. Other criteria include influence of situational limitations, choice space, sensitivity to views of analysts and influence on results.

An alternative approach to the use of SoK judgements is to perform judgements of the importance or criticality of the justified beliefs that form the knowledge basis K. As knowledge is justified beliefs (often formulated as assumptions), such judgements would be a useful supplement to the probabilistic metrics. The importance (criticality) is assessed by considering errors in these beliefs (deviations of the assumptions made), the implications for the quantities studied in the probabilistic analysis and associated uncertainties. The uncertainties are judged by a direct argument or by using probability with related strength of knowledge judgements. All judgements here are of a qualitative form. See Section 4.2.4 for an example of this approach.

As the IPCC case demonstrates, the scientific findings of climate change are strongly intertwined with judgements of the strength of the knowledge supporting these findings. Although there are weaknesses in the IPCC framework for uncertainty and risk treatment, the use of confidence statements in the IPCC setting is a step in the right direction. A lot of scientific work lacks this type of consideration. Results have been and are still produced without stressing that these are conditional on some knowledge, and this knowledge could be more or less strong and even erroneous. Critical assumptions are commonly reported as an integrated feature of the results, but more comprehensive knowledge assessments as discussed in this section are more seldom

carried out. If we also include potential surprises relative to this knowledge, as will be discussed in the following, they are even more seldom conducted. The scientific literature on uncertainty and risk analysis has devoted little attention to this type of issues, and there is no established practice on how to deal with them.

The potential for surprises: black swans

As discussed in Section 2.2, knowledge can be considered as justified beliefs. Hence, knowledge can be more or less strong and also erroneous. Experts can agree and the data available generate beliefs as formulated above in the IPCC case. Yet, there is a potential for surprise; the knowledge can be wrong.

Dealing with this type of risk is challenging, as it extends beyond the knowledge available. Nonetheless, it is an essential component of science, of a type that forces scientists to balance confidence with humility, as discussed in Sections 3.1.3 and 3.2.3.

There are different types of surprises. One of the most important ones is unknown knowns, as reflected by the origin of the black swan metaphor. Before the discovery of Australia, people in the Old World believed all swans were white; then, in 1697, a Dutch expedition to Western Australia discovered black swans (Taleb 2007), a surprise for us, but not for people living there. The September 11 event is an example of an unknown known. It came a surprise to most of us but, of course, not to those planning the attack. Many unknown knowns can be revealed by proper analysis, but, in practice, there will always be limitations, and surprises of this type can occur. Unknown unknowns – events not known to anybody – are more challenging to identify, but fortunately such events are rarer. Testing and research are generic measures to meet this type of events, as well as a focus on resilience, signals and warnings (Aven 2015b).

The third category of surprises is of a different type. In this case, the event is known but not believed to occur because of low judged probability (Aven 2015b). To illustrate the idea, think about an event A, for which a knowledge-based probability of 0.000001 is assigned given the knowledge K, that is $P(A|K) = 0.000001$, or we could think about a situation where an imprecision interval is instead specified: $P(A|K) < 0.000001$. The point is that the probability is judged so low that the occurrence of the event is ignored for all practical purposes. Now suppose the probability assignment is based on a specific assumption, for example that some potential attackers do not have the capacity to carry out a type of attack. Given this assumption, the probability is found to be negligible. Hence, if the event occurs, it will come as a surprise given the knowledge available. However, the assumption could be wrong, and, clearly, with a different knowledge

base, the probability could be judged high, and the occurrence of the event would not be seen as surprising.

This discussion relates to the fundamentals of risk assessments. Current practice has, to a large extent, been based on a frequentist understanding of probabilities, seeing probability judgements as reflecting states of the world. In this view, it is believed that an event with an estimated probability will occur sooner or later; it is like a physical law. However, this 'destiny perspective' on probability and risk is not very meaningful or fruitful for assessing and managing risk in cases with a potential for extreme outcomes and large uncertainties. Yet, this type of thinking prevails, to a large extent, in university programmes, particularly in engineering and business. The risk and uncertainty analysis sciences have not yet been able to challenge this thinking in a way that has changed common practices.

4.2.3 The full risk characterization (C',Q,K)

Combining C', Q and K gives a risk description or characterization. The format of this characterization has to be adapted to the concrete case considered and the need for decision support. Often metrics are introduced, linking consequences and probabilities, for example f-n curves showing the probability of an accident with at least n fatalities or an expected number of fatalities in a population. The suitability of these metrics is always an issue, especially when it comes to the use of expected values, as commented on earlier several times. In any case, the knowledge dimension needs to be reflected and particularly the strength of this knowledge, as highlighted above.

The term C' can be a quantity in real life, for example the time to failure of a specific system, or it could be a model quantity like the occurrence rate λ in the above Poisson model, the 'true' quantity defined as the average number of events occurring for the period considered if we could hypothetically repeat the situation over and over again infinitely. Or it could be the model error $M_e = F - h$, where h is the true variation in a population being studied and F the probability model used to model h.

To characterize the uncertainties about the unknown quantities C', three basic elements are needed:

1) Knowledge-based (also referred to as a subjective and judgemental) probabilities P or related interval (imprecision) probabilities
2) A judgement of the strength of the knowledge K (SoK) supporting these probabilities
3) The knowledge K.

We write for short (P,SoK,K). A knowledge-based (imprecise) probability P of an event A is interpreted with reference to a standard, as explained in Sections 3.1.1 and 4.2.2.

4.2.4 Use of the risk conceptualization framework: Two examples

In this section, we consider two applications of the framework. The first one highlights risk matrices and related risk characterizations. The second looks into assumptions and risk (influencing) factors, with related considerations of importance for risk management and decision-making.

Risk matrices: National and global risk characterizations

We return to the use of risk matrices, following up the discussion in Section 1.2. Risk matrices have been strongly criticized, yet they are still used extensively in practice, for example for characterizing national and global risks (see e.g. Aven and Cox 2016) and the references therein. In this section, we will specifically address the approach taken by the World Economic Forum in their Global Risk Report (WEF 2018; refer to Section 1.2). The aim of their work is to reveal the highest risks on the basis of a survey of a number of competent people. The current approach highlights the likelihood-impact dimensions and uses risk matrices to visualize the risk level. As discussed in the previous sections (see also Aven and Cox 2016), this approach can be improved by better reflecting the knowledge dimension.

In the following, we present a concrete suggestion for how this can be achieved.

Our concern is global risk events, defined as events resulting in a significant negative impact for several countries or industries within the next ten years (WEF 2018). What is meant by 'significant' in this respect is not made clear, but we refer to it here as events affecting the life and health of a large number of people, or leading to considerable environmental damage, or having other severe impacts related to something that humans value. Examples of such events include (WEF 2018): asset bubble in a major economy, extreme weather events, food crises and terrorist attacks, all of which have significant impacts.

Let A be such an event and let P(A|K) be the probability assignment of A, given the assessor's knowledge basis K, and SoK his/her associated strength of knowledge judgement, using, for example, the categories strong (3), medium (2) and poor (1). For the probability assignments, we can use predefined categories like 0.999 ($\geq$0.995), 0.99 (0.995–0.95], 0.90 (0.95–0.75], 0.50 (0.75–0.25], 0.10 (0.25–0.05], 0.01 (0.05–0.005] and 0.001 (<0.005).

If we have n persons conducting this assignment, we can report the average value of P and an interval covering 90 per cent of the assigned probabilities. In addition, we would compute an average strength of knowledge figure. Considering the whole sets of events A, we can group them according to probability and SoK. The events with the highest judged risk are those with high probability and low SoK value. We can also make a scatter plot with the sample points for these two dimensions, showing the variations and features of these two dimensions for the n persons.

In this characterization, we have fixed the consequence (impact) dimension, which simplifies the analysis and eliminates imprecision problems related to the type of events for which the probability assignments are to be applied. If we had defined the risk event by, for example, "extreme weather event", a clarification of what this event means would have been necessary, and the assessor would also have had to specify the impacts in some way, given the occurrence of this event. Certainly, if this specification had been restricted to some expected values, the analysis would have lost information value in relation to the possible occurrence of significant impacts, which is really the type of event of interest for this study.

This does not mean that such matrices – focusing on the initial events – cannot be informative in other cases. However, when choosing such an approach, it is essential that the events are precisely defined, that we consider not only the expected consequences (impacts), given the occurrence of events, but also the spectrum of possible consequences, as well as the strength of knowledge supporting the judgements of the probability-related judgements. A 90 per cent prediction interval may, for example, be used for the consequence dimension, i.e. an interval which covers the quantity of interest with 90 per cent probability. In this way, an extended risk matrix is generated, in which, for example, colours can be used for reflecting strong, medium or poor strength of knowledge, see e.g. Aven and Renn (2015) and Section 5.5.2.

In addition to an analysis like this covering A,C,P and SoK, a checklist is provided, as in Bjerga and Aven (2016), to highlight potential surprises relative to the analysts' knowledge (so-called black swans):

i. The possibility of unknown knowns (i.e. others, but not the analysis group, have the knowledge). Have special measures been implemented to check for this type of event (for example, the use of an independent review of the analysis)?
ii. The possibility that events are disregarded because of very low probabilities, although these probabilities are based on critical assumptions. Have special measures been implemented to check for this type of event (for example, signals and warnings influencing the existing knowledge basis)?

iii. Risk related to deviations from assumptions made
iv. Changes of knowledge over time

To rank risk events on the basis of the three dimensions of probability, impact and knowledge is difficult. The following approach has been suggested (Aven and Flage 2018):

1. Very high risk: potential for extreme consequences, relatively large associated probability of such consequences and/or significant uncertainty (relatively weak background knowledge)
2. High risk: potential for extreme consequences, relatively small associated probability of such consequences and moderate or weak background knowledge
3. Moderate risk: between low and high risk. For example, the potential for moderate consequences and weak background knowledge.
4. Low risk: no potential for serious consequences.

For the risk management, such a ranking is, however, not essential. The point is rather that the various features of the risk events have been highlighted and summarized, and this can be done without transforming the information to a one-dimensional scale. Judgements are needed in any case.

Criticality rankings of assumptions and risk factors (sources)

We consider an example from the oil and gas industry, based on Veland and Aven (2015). In the example, a large hydrocarbon leakage occurred on an offshore installation, with the potential for a major accident. The leakage occurred inside a vertical passageway shaft located in one of the concrete legs of the installation. The leakage occurred during modification work. A special tool (a hot tap machine) was used to contain the hydrocarbon fluids while performing the work. This machine had been modified to be able to perform the work. The leakage resulted in evaporation of hydrocarbon gas and created an explosive atmosphere inside the shaft. The accident reports following the incident pointed to poor risk understanding as a result of many issues, including:

- Prior to the event, it was assumed that hardly any gas would evaporate from a possible oil leakage, the argument being that the medium was stabilized oil. Hence, it was believed that an explosive atmosphere would not be reached inside the shaft, and it was consequently decided not to prepare a specific emergency response plan for the situation.

- Some of the key personnel working on the installation – personnel who had extensive knowledge and experience relevant to the operation – did not attend the safety job analysis group meeting.

In this example, we have two critical justified beliefs (assumptions):

JB1: hardly any gas would evaporate from a possible oil leakage

JB2: new technology for the top machine was as safe as the traditional

An important risk factor (source) is the personnel conducting the job safety analysis and their competence and insights.

Let us make a thought construction going back in time, and a risk assessment is to be conducted prior to the modification work. The assessment focuses on events, consequences and probability but includes in addition an evaluation of the importance of assumptions and risk sources.

First, a list of the assumptions made is identified. This work is in itself challenging, as assumptions can be more or less tacitly formulated. The next task is then to perform a qualitative risk assessment of these assumptions, highlighting

– Deviations from these statements (assumptions)
– Implications of such deviations
– Judgements of probability
– Related strength of knowledge

A ranking is conducted with categories: high, medium and low associated risk. If an assumption is assigned a high-risk score, it is to be followed up to see how the risk can be reduced. Attention should also be given to the assumptions labelled medium, if the number of high scores is not too great. In the concrete case, by asking questions like:

– Do we understand the phenomena involved?
– Have we evidence supporting our judgements?
– Have our beliefs been checked by others?

it is likely that critical questions would have been raised concerning the validity of the assumptions made. That in itself could have been enough to involve other personnel in the assessment, who had stronger knowledge about the relevant phenomena and processes being studied.

Given a high-risk importance score, the jump to measures which can reduce the risk is quick, as we see from this example. In this case, the knowledge aspect of risk was the key to reducing risk, since, as seen from the

outside, the analysis group had poor knowledge. From the group's perspective, the risk was considered low and under control. The assigned probabilities were low, but the supporting knowledge could be questioned. And that is exactly what the suggested methodology intends to do: highlight more strongly the criticality of the knowledge that forms the basis of the probability judgements.

In addition, risk (influencing) factors (sources, drivers) are listed and a crude qualitative analysis is conducted to identify the most important ones. Such underlying factors are often identified in relation to cause analysis of initiating events (using fault trees or Bayesian networks) but could also be revealed by a simple brainstorming session in the analysis group. The key question to answer is: what are the elements (systems, components, persons, events, situations, etc.) that generate the potential severe scenarios and consequences? In the example, the competence of the personnel taking part in the safety job analysis was identified as such a factor. It is rather a general factor, applicable to all types of risk assessment.

Next, an assessment of the importance of these factors is conducted. We ask: how sensitive is the risk to changes in the risk factor? And to what extent is the risk factor present (degree of exposure, probability)? In addition, we need to consider the strength of knowledge on which these judgements are based. In our example, an assessment of the sensitivity would give a rather high score, as it is acknowledged that the understanding of the phenomena and processes studied is very much dependent on the personnel's competence and insights, related to technical aspects linked to the new machine and process safety. The exposure is high, as the assessors' competence and insights influence the risk assessment throughout its execution. Hence the factor is assigned a high importance score, and measures should be implemented to reduce the risk contribution from this factor. Many measures could be thought of in this example, but the obvious one is to look for personnel with specific competence, insights and experience related to the issues studied.

4.3 DISCUSSION

4.3.1 Do we need to characterize the risks?

The previous sections have presented simple ways of characterizing risk in practical settings, supplementing and adding new features compared to the current methods such as risk matrices and other loss-probability-based metrics. Some links were made to risk management and decision-making, and one can always argue that what is actually implemented is what is important and not the risk assessment per se. The point being made is that in

many cases we can skip the detailed risk characterizations and go directly to the risk-reducing measures and the decision-making, as in, for example, Lambert et al. (2012) and Karvetski and Lambert (2012). What measures are needed to make the activity safe? Acknowledging that there is no number that defines what safe means, the focus should be on the identification and assessment of measures that can ensure acceptability and improved safety.

This type of argumentation can be justified to some degree. In many cases, the issue is really to look for measures that can improve safety and eventually make the activity safe enough. Identifying risk influencing factors and performing a qualitative ranking to identify the most critical ones, for example in line with the ideas of Section 4.2, is often sufficient in operational safety contexts with a culture and economic conditions which allow measures to be effectively implemented when identified. However, in practice, there are always limitations. In the offshore example, it is easy with hindsight to conclude that the risk assessment should be open to broader involvement from external personnel groups to improve the knowledge basis. Prior to the modification, there is, however, a need to justify the increased uses of resources. If the problem had been related to only one activity, it would not have been difficult to solve, but there could be thousands, and a change in the routines, requiring in general broader analysis groups, could be costly. The need to justify the measures arises.

4.3.2 Assessing assumption deviation risks

As commented in Bjørnsen and Aven (2016), in accident reports, for example for the offshore case considered here, the point is commonly raised that the risk understanding was poor, as key assumptions or beliefs were wrong. However, what can we learn from such an acknowledgement? There is no guarantee that all the assumptions in a risk assessment are correct. Rather, the issue should be: does the risk assessment, in a rational and fruitful way, focus sufficiently on the risk related to deviations in such assumptions and beliefs? Some practical guidelines for how to obtain improved assessment in this respect are presented in this chapter. The key is to see beyond loss-likelihood: to always think about knowledge and potential surprises relative to this knowledge. By doing this, we cannot guarantee that erroneous assumptions and beliefs will not be made, but the associated risks are reduced.

4.3.3 The need for a semi-quantitative approach

The approaches argued for above mean a semi-quantitative approach to risk assessment. It is acknowledged that risk cannot be characterized by numbers alone. For many analysts, this means a less precise analysis and lack of traceability, as quantification is superior to qualitative analysis on these points.

For some analysts, it also means more subjectivity, as they consider quantification less subjective than qualitative analysis. However, choosing a pure quantitative approach brings challenges in relation to properly representing and treating all types of risk and uncertainties, as thoroughly discussed in the literature (e.g. Aven 2012a) and also to some extent in this book. The problem is, thus, either stick to a quantitative approach, which has strong limitations, or adopt a combined quantitative-qualitative approach, which seeks to meet these limitations. The present book argues that, in reality, there is no alternative to the latter approach. See also discussion in Section 3.1.

4.4 SUMMARY AND CONCLUSIONS

This chapter has presented a framework with some examples of how risk should be understood and characterized, improving current approaches and methods. The main challenge has been to better incorporate the knowledge dimension of risk. This dimension is not properly reflected when restricting risk to consequences and probability. The following list highlights some main points:

1) Risk = Consequences of the activity and related uncertainties (Risk = (C,U)).
2) In risk assessment, the risk is characterized by some specified consequences C' and an uncertainty measure (interpreted in a wide sense) Q, in addition to the knowledge K supporting C' and Q. Knowledge is here understood as justified beliefs. Thus, in generic terms: Risk characterization = (C',Q,K).
3) The default implementation of the uncertainty measure Q is that it covers probability (interval probability) (P) and strength of knowledge judgements (SoK). Hence, Q = (P, SoK).
4) Q is used for all types of unknown quantities, observables or parameters of probability models.
5) As the knowledge can be more or less strong and also erroneous, the risk assessment also needs to examine K, to identify potential surprises.
6) Risk matrices in the traditional two-dimensional consequences-probability form should not be used. A third strength of knowledge dimension should always be included, resulting in an extended risk matrix. The consequence dimension also needs, in general, to capture the spectrum of consequences, not only the expected value, given the initiating event. A prediction interval can be used for this purpose. Often, it may be useful to fix the consequence dimension to a defined type of outcome, for example events with some minimum damage.

7) A simple method for criticality ranking of assumptions is presented, based on a broad risk characterization of deviations in these assumptions (Section 4.2.4).
8) A simple method for criticality ranking of risk (influencing) factors is also presented (Section 4.2.4), highlighting the sensitivity of changes in these factors, with respect to the risk description and the degree of exposure (probability) to this factor. A factor, for example a type of load, may quickly lead the risk numbers to increase when the activity is exposed to this load, but, if the loading is rare, it may not be critical.

The framework and related methods aim to guide risk analysts and practitioners working with risk on how to perform a simple assessment of risk and to characterize risk, in order to properly inform decision-makers.

5 Risk assessment

Reference is made to Section 3.1.1, where risk assessment is defined as: the systematic process to identify risk sources, threats, hazards and opportunities; understanding how these can occur and what their consequences can be; representing and expressing uncertainties and risk; and determining the significance of the risk using relevant criteria. Some main principles for ensuring high-quality risk assessment are summarized in Section 3.1.1. The risk assessment aims at understanding and characterizing risk, in order to support decision-making related to risk (including making judgements about acceptability and choosing among alternatives). The assessments help us identify what might go wrong, why and how it might go wrong; what the consequences are and how bad they are. Risk assessment is in many ways an established approach, with suitable methods and models for responding to such questions and issues, founded to a large extent on probabilistic and statistical thinking and tools; see, for example, Bedford and Cooke (2001), Vose (2008), Meyer and Reniers (2013), Aven (2015e) and Haimes (2015). Risk assessment is extensively used in practice, addressing all types of applications, including health and safety issues, engineering and finance.

As such, risk assessment is recognized as a useful practical tool. However, when it comes to the scientific quality of risk assessment, there are still many issues raised. We will look into some of these in this section. We first focus on the reliability and validity concepts introduced in Section 3.1.1. When discussing the quality of a risk assessment, a basic question is the degree to which the risk assessment is able to adequately characterize the risk. A main challenge is uncertainties, and different strategies are used in practice to meet it, including conservatism, which is the topic of Section 5.2. Models play an important role in risk assessments, to understand and characterize risk, in particular on issues concerning cause–effect relationships (for example, is a specific type of exposure dangerous?). Section 5.3 discusses the topic and explains what is meant by model uncertainties. Modelling means

that simplifications are made in the assessments. Section 5.4 looks closely into one category of such simplifications: potential scenarios and events are ignored, either because they are not identified or due to low probability. The final Section 5.5 follows up item 11 in Section 3.1.1 and discusses the difference in perspective between the analysts and the decision-makers. When the issue is the quality of the risk assessments and the risk characterizations in particular, it is essential to understand that decision-makers normally need to have a broader view on risk than is the scope of the risk assessment. The limitations of the risk assessments are as important as the produced risk metrics and descriptions.

5.1 RELIABILITY AND VALIDITY

As mentioned in Section 3.1.1, the concept of reliability is concerned with the consistency of the 'measuring instrument' (analysts, methods, procedures), whereas validity is concerned with the success at 'measuring' what one set out to 'measure' in the analysis. The concepts are commonly visualized by illustrations, as in Figure 5.1, which is based on the idea that we have repeated measurements (x) of a quantity, whose 'true' value is represented by the circle centre. Reliability is obtained if the measurements are close to each other, whereas validity is ensured if the measurements are close to the centre. It is also common to consider validity expressed by the average measurement. In that case, the measurements could show large spread but, as long as the average is close to the centre, validity is ensured.

5.1.1 The traditional statistical framework

At first glance, and in view of Figure 5.1, these concepts seem to be rather unproblematic for use in risk assessment too. For a traditional statistical

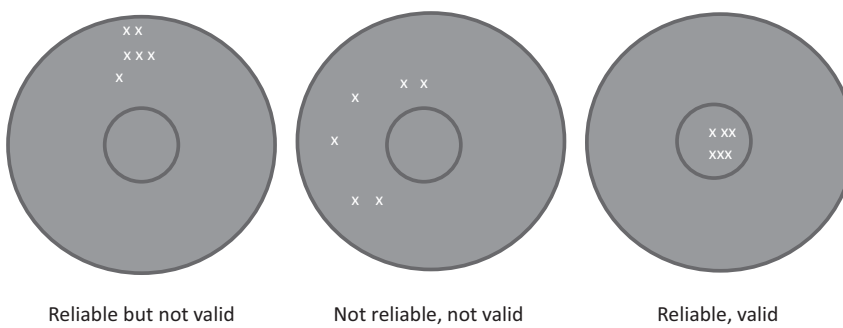


FIGURE 5.1 Traditional illustrations of the concepts of reliability and validity

framework, they are. Let q be the frequentist probability that an arbitrary chosen person in a huge population has a specific property D (for example, suffers from a specific disease). By repeated samples of measurements, reliability and validity are obtained. Repeated sample estimates, based on a sufficiently large number of observations, show consistency (reliability) and accuracy (validity) relative to the true underlying q value. Textbooks in statistics address this set-up, which will not be discussed in more detail in this book.

5.1.2 Broader frameworks

However, if we look into situations which extend beyond this standard statistical framework, these concepts are not so easily interpreted. To illustrate, suppose a risk assessment conducted by an analyst team T_1 produces a probability $P_1(A)$ of an event A. Suppose another team T_2 conducts a risk assessment of the same activity or system and derives a probability $P_2(A)$. Now, does the concept of reliability express that the two probabilities should be approximately the same for the two teams? Yes, this would be a possible interpretation of the reliability criterion. However, it is a problematic one. Using the terminology of Section 4.2, we can write $P_i(A) = P(A|K_i)$, for i equal to 1 and 2, where K_i is the knowledge that the probability is based on for team i. In general, it does not seem meaningful to require that these two probabilities should be the same, as the background knowledge could be different. If, however, the knowledge K is basically the same for the two teams, intuitively also the probabilities should be the same. Unfortunately, uncertainty assessments are not so straightforward, as was discussed in Section 4.2. Even if K is the same, there is no guarantee that the corresponding probabilities are the same. The transformation from the knowledge to the probabilities represents a step which reflects the assessor's judgements. More objective transformation processes can be derived, leading to probability intervals, as addressed in Section 4.2.

Thus, the concept of reliability has to be seen in relation to the aim of the assessment. If the risk results are to express the assessors' judgements given their knowledge, we have to acknowledge that the risk metrics of the form P(A|K) may strongly depend on both the background knowledge K and the assessors making the probabilistic judgements. Reliability in this case is more about ensuring that consistency is ensured when, for example, rerunning the computational methods. It is also essential to document the relevant argumentation for the specific probability assignments made.

If, on the other hand, the aim of the risk assessment is to obtain 'objective' representations of uncertainty given a specified knowledge, we are led to interval probabilities. Through this approach, a stronger degree

of consistency is obtained, in the sense that we should be led to the same risk representations, given some specified knowledge. See discussion in Section 4.2.2.

In general, the validity criterion relates to the degree to which the risk assessment describes the specific concepts that one is attempting to describe, the degree to which one is able to assess what one sets out to assess. Alternatively, validity may just suggest that the assessment is solid, in some sense, meeting some relevant criteria.

Chapter 4 discusses issues of relevance for this discussion. The risk assessment aims to adequately describe risk, and the validity criterion reflects the degree to which the assessment actually does this. Then, we are led to discussions about the suitability of risk metrics, based on probabilities and expected values. It is argued in Chapter 4 that such metrics in general have strong limitations, and risk assessments that describe risk using such metrics alone are not valid; they do not very well describe what they set out to describe: namely, risk.

5.1.3 Describing risk using a knowledge-based probability

Consider a probabilistic risk assessment, which produces output in the form of a knowledge-based probability P for an event A. This probability expresses the analysts' degree of belief that the event A will occur, given some background knowledge K. We write P(A|K). This knowledge is essentially justified beliefs, founded on data, information, models, testing, argumentation, etc. The probability as such cannot meaningfully be validated, as it is a subjective or intersubjective instrument to express uncertainties, and there is no true objective reference against which to compare it. However, it is possible to establish criteria for the process of making such judgements. These can relate to K and the process of transforming K to P. For example, if the background knowledge K is weak, it can be argued that the probability assignment P does not have a solid foundation and, hence, the assessment is not valid. Another example would be that the transformation process from K to P in some cases has strong limitations, as the use of probability forces the analysts to add information that is not really present in the data available; see discussion in Section 4.2.2.

5.1.4 Is validity about scientific quality or meeting the decision-makers' expectations?

More generally, the issue of validity would question the events and quantities of interest, the choice of uncertainty measure, the strength of the background knowledge, as well as the process of transforming this knowledge

into suitable risk metrics and characterizations. For this purpose, we can formulate criteria on a general basis from a scientific risk analysis perspective, as indicated above, but equally important is the quality of the risk assessment, as seen from the users' perspective. How credible are the results from the view of the different stakeholders? Are they trustworthy? The choice of metrics should obviously meet the needs of the decision-makers. It is tempting to state that the quality of the risk assessment is mainly determined by its ability to meet the decision-makers' expectations. However, such a perspective is easily refuted. The decision-maker can be satisfied with a risk assessment expressing a low probability number for an extreme event, without giving weight to the knowledge supporting it or the process for deriving this number. The quality of K and this process are obviously essential elements of the assessment. As highlighted above, the scientific quality is the key to ensuring validity.

As another example to illustrate this point, consider an analyst team which produces risk numbers in the form of expected values. The decision-makers and other stakeholders could find that the assessment meets their needs but, surely, such an approach would in most cases not be able to properly express risk from a scientific point of view, as risk is more than expected values, see Section 4.2.

5.1.5 The quantities of interest – observables or probabilistic parameters?

Validity is also about addressing the right quantities in a different sense. Is the quantity of interest a parameter of a probability model or an observable quantity? Providing clear interpretations of all quantities of interest is a well-known rule for clarifying what should be focused on in the analysis. The key question is often whether we like to address averages in populations – real or thought-constructed populations – or a specific unit. In general, risk assessment should seek to focus on observable or potential observable quantities and not on fictitious parameters with no clear interpretations. Models using unobservable parameters could be used as a tool for gaining insights about the observable quantities, as we see, for example, in Bayesian analysis (Lindley 2000).

5.1.6 From accurate risk estimation to risk knowledge generation

The validity issues lead us to the question of whether risk assessment can be used to accurately estimate risk. Surely, if accurate estimation – as well as accurate prediction – is a requirement, risk assessment is not in general valid, as commented in Section 1.3. In cases of large uncertainty, such estimation

and prediction cannot be ensured. Risk assessment in general does not meet the criteria of the traditional scientific method. However, by considering risk assessment as a tool for knowledge generation – as a systematic process to comprehend the nature of risk and to express and evaluate risk – a new perspective on risk assessment is obtained. It is always relevant. It does not of course mean that all problems of risk assessment are removed, but the problems are of a different type. It is still a challenge to transform knowledge K to a suitable risk characterization and deal with potentials for surprises. Yet, the current methods represent the best knowledge of the risk analysis field and science.

5.1.7 Example 1.2 Continued (see also Section 4.2.4) – Global and national risks

Section 4.2 and the above discussion have shown that approaches based on expected values and probabilities, E[C] and (P,C), fail to meet the validity criterion, as important aspects of risk are not captured. There are, however, also challenges when using the (C,U) approach. Clearly, with hard data alone, risk in relation to serious events will not be well described. The use of expert judgements is more meaningful. However, the study requires that events are precisely defined, to reduce ambiguity when experts are to make their judgements. Let B be a well-defined event, for example an event expressing more than 1,000 fatalities. If several experts express this probability, a mean value can be computed, to represent the judgements of the experts as a group. Alternatively, the mean could be seen as the analyst's judgement on the basis of the experts' input. In addition, scatter plots should be used as mentioned in Section 4.2.4, with the sample points for P and SoK showing the variations and features of these two dimensions for the experts' judgements.

The risk characterizations obtained by such expert judgements have to be interpreted for what they are: judgements about risk conducted by a group of experts. The results will depend on the experts included, and there could also be measurement issues, as thoroughly discussed in the literature, for example as a result of biases (heuristics) in people's ability to use probability numbers to reflect uncertainties (see e.g. Kahneman et al. 1982, Rohrmann and Renn 2000, Renn 2008).

Different groups of experts should be used to check how sensitive the results are, with respect to who are included in the study. In theory, it would also be interesting to use the approach to compare judgements made by different types of experts, for different regions, etc. However, care has to be shown when interpreting the results and differences, so that noise is not mixed with more fundamental differences in judgements among

different groups. Suitable statistical analysis techniques should be applied for this purpose.

Risk assessments, based on modelling of relevant phenomena, are applicable for some types of events but not so much for situations characterized by large uncertainties. If phenomena are difficult to model because of lack of knowledge, such risk assessments would not give much insight into global or national risks, compared to more direct approaches based on expert opinions. Rather, the risk assessments conducted should be seen as input to the expert judgements made.

Hard data and risk assessments based on modelling of relevant phenomena provide information that can be used in risk assessments founded on expert judgements. To be able to reflect changes and trends, and the potential for new types of events and surprises, expert judgements are required. The approach outlined above and in more detail in Section 4.2.4, with a focus on some specific serious events, with judgements of probability and strength of knowledge, will capture essential aspects of risk, and the issue is more about how to select experts and train them in the assignment processes. Probability is a challenging concept, and efforts should be made to give all assigners a common understanding of what a probability of say 0.2 means in this context. Many people would relate the probability concept to frequency of events, but such an interpretation would not be feasible in this case. Rather, the idea is to use probability to express uncertainties and degree of belief, as is explained in Section 4.2 when referring to the urn comparisons. The training of assessors to make probability assignments according to such an interpretation needs to be an integrated part of the risk assessments, as it is a skill that needs to be developed. Lack of training of the assessors means that unnecessary noise is introduced into the study.

5.1.8 Black swans

Finally, a comment on potential surprises and the unforeseen – 'black swans'. These events represent a challenge, as they come as a surprise, relative to our knowledge. Knowledge is basically justified beliefs (SRA 2015a), and this knowledge can be more or less strong but also wrong or erroneous, and this represents a challenge in risk characterizations and management. For obvious reasons, it is not possible to show or present the related risks as a part of the risk descriptions, but we can and should highlight the knowledge on which the judgements are based and, in particular, the assumptions made. Addressing and discussing this knowledge and these assumptions is, in many cases, equally important as, if not more important than, highlighting the probabilities derived. See Aven (2019d) for further discussion of this example (Section 5.1.7). We return to the issue of surprises in Section 5.4.

5.2 CONSERVATISM IN RISK ASSESSMENT

It is common to use conservatism in risk assessments, replacing uncertain quantities with values that lead to a higher level of risk. It is argued that the approach represents a practical method for dealing with uncertainties and lack of knowledge in risk assessment. If the computed probabilities meet the pre-defined criteria with the conservative quantities, there is strong support for the 'real risk' of meeting these criteria. In this section, we look more closely into this practice, the main aims being to clarify what it actually means and what the implications are, as well as providing some recommendations. It is argued that conservatism should be avoided in risk assessments – 'best judgements' should be the ruling thinking, to allow for meaningful comparisons of options. By incorporating sensitivity analyses and strength of knowledge judgements for the background knowledge on which the assigned probabilities are based, the robustness of the conclusions can be more adequately assessed.

5.2.1 What is the issue?

In quantified risk assessments, various probability-based metrics are computed, for example the probability of at least n fatalities or the probability that a fixed but arbitrary person in a population shall be killed due to an accident or the expected number of fatalities for a specific group of people, during a defined period of time. Let y denote such a metric. To compute y, models are developed and a number of assumptions made, for example that: a wall will withstand an explosion pressure of 1 bar; in the case of an ignited gas leakage, 1 person will immediately be killed; the reliability of a safety system is 0.95, etc. Hence y is dependent on a number of quantities, for example the strength of the wall (s), the number of people that will immediately be killed in the case of an ignited gas leakage (n) and the reliability of the safety system (q). These quantities are assumed known – here 1, 1 and 0.95, respectively, but the choice is not always straightforward, as these quantities are unknown, subject to uncertainties.

In practice, quantified risk assessments cannot be conducted without making such assumptions, and the issue of how to make these assumptions is thus highly relevant. However, the interpretation is not always clear. Commonly, a link is made to overestimation of the risk, which means that the estimated risk is higher than the 'best estimate' of the risk. Conservative assumptions are justified with reference to cautionary thinking. Rosqvist and Tuominen (2004a) highlight this when stating that, with respect to risk, conservative modelling assumptions are preferred to optimistic ones, in order to ensure that the system does not falsely satisfy an acceptance criterion (a threshold risk level).

But what does the concept of conservatism in risk assessment really mean? The above analysis seems to indicate that the concept is easily explained, but there are issues that need to be examined more closely, particularly concerning the *level* of conservatism. To illustrate this, suppose that there are considerable uncertainties about n in the above example and the number is increased to 2 in order to be conservative. But why not 3 or 4? If an uncertainty analysis had been carried out for n, a probability distribution of n could have been assigned, say 0.4, 0.3, 0.2 and 0.1, for n = 0,1,2 and 3, respectively, and the question about how conservative n = 2 really is can be raised.

Secondly, we need to clarify how conservatism relates to the strength of the knowledge on which the probabilities are based. A risk description is defined through the risk metrics but also the knowledge and strength of knowledge that support the probability judgements. If we replace n by 2, does the strength of knowledge increase or decrease?

Thirdly, we need to question the usefulness of conservatism in the practical decision-making processes. Risk assessment is not only about verification in relation to acceptance criteria; equally important is its use to compare options with respect to risk. Clearly, for such a purpose, the conservatism could hamper the appropriate use of quantified risk assessments. We question what is really gained by conservatism – is not sensitivity analysis able to give the same input to the decision-making?

The issue of conservatism in safety management has been discussed in many contexts, for example in the nuclear industry in the late 1990s in the US, in relation to the use of traditional safety analysis methods based on deterministic requirements and safety margins (in line with the defence-in-depth principle and other cautious policies to meet the risk and uncertainties). Quantitative risk assessments are introduced to supplement these analysis methods and avoid 'unnecessary conservatism'. The key is to be properly risk-informed (see e.g. Apostolakis 2004, NRC 2009). The present analysis addresses the issue of conservatism in the way risk is assessed and how this risk information is presented to the decision-makers, and it is argued that this type of conservatism is problematic and should be avoided.

To discuss these topics, a formal risk assessment set-up will be introduced.

5.2.2 A formal set-up

In quantified risk assessments (QRAs), a set of probability-based risk metrics are defined, such as the probability of specific events (for example, at least n number of fatalities or the impairment of some defined safety functions) or some expected values (for example PLL, the expected number of fatalities in a year). These metrics are computed on the basis of some models, typically event trees and fault trees, as well as more technical models based on physical representations of phenomena like fire and explosions.

Let y denote such a metric, and let x be a vector of parameters of the total model f used for computing y. Hence, we can write

$$y = f(x).$$

To illustrate the set-up, a simple example will be used (based on Aven 2012c). See Figure 5.2. The model is an event tree with initiating event "major gas leakage" and two branching events: B: ignition and C: explosion. Depending on these events, the outcome is 2, 1 or 0 fatalities, as shown in the figure. Let p_1, p_2 and p_3 be (frequentist) probabilities of the events A, B and C, respectively, where it is understood that B is conditional on the occurrence of A, and C is conditional on the occurrence of A and B. Furthermore, let r denote the (frequentist) probability of two fatalities. Then the event tree model states that

$$r = p_1 \cdot p_2 \cdot p_3$$

In the risk assessments, estimates (denoted $*$) of the quantities are produced, leading to

$$r^* = p_1^* \cdot p_2^* \cdot p_3^*$$

An alternative way of expressing the risk is to start from Figure 5.2 and the event tree model there, and use knowledge-based probabilities P to express the uncertainties related to the events A, B and C, to obtain

$$P(Y=2) = P(A) \cdot P(B|A) \cdot P(C|A,B).$$

The underlying model giving this probability takes the form

$$I(Y=2) = I(A) \cdot I(B) \cdot I(C),$$

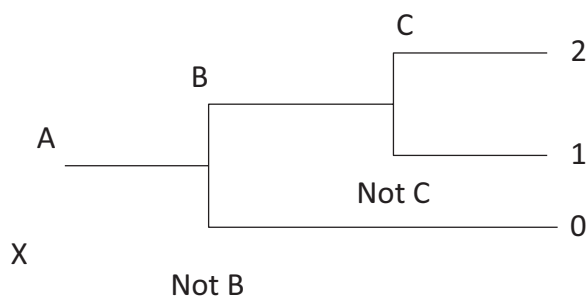


FIGURE 5.2 Event tree example. A: major gas leakage, B: ignition, C: explosion, X: number of leakages (based on Aven 2012c).

where I is the indicator function, which is 1 if the argument is true and 0 otherwise.

In the former frequentist case, y corresponds to r*, and x to $p^*=(p_1^*, p_2^*, p_3^*)$, whereas, in the alternative case, y corresponds to P(Y=2), and x to (P(A), P(B|A), P(C|A,B)). The function f is defined by $f(x) = x_1 \cdot x_2 \cdot x_3$ in both cases.

The metric with its model is based on a set of assumptions. Two examples in the case of Figure 5.2 are:

a) The number of fatalities is 2 if the events A, B and C occur
b) The number of leakages in the period considered is 1.

Let $z = (z_1, z_2, \ldots z_m)$ denote the vector of assumptions made. Then we can write

$$y = f(x|z),$$

where f(x|z) denotes the function f given the assumptions z. In both cases, we use the risk assessment to support decision-making on comparing options and to make judgements about risk acceptability/tolerability.

Using this set-up, in the coming section we will discuss what conservatism in risk assessment means. For this purpose, we will rewrite the set-up slightly.

Assume we can write z_i as a function of a parameter u_i, so that we can write $z_i = z_i(u_i)$. Consider the a and b examples above and let us refer to them as z_1 and z_2, respectively. Then we may write a as $z_1(u_1) = u_1 = 2$ and b as $z_2(u_2) = u_2 = 1$, where u_1 expresses the number of fatalities if the events A, B and C occur and u_2 is the number of leakages in the period considered. We see that the risk metric y is an increasing function in each u_i, meaning that increased values of the assumption parameters lead to higher risk, according to the metric used.

Introducing the vector $u = (u_1, u_2, \ldots u_m)$, we can also write y as a function of u, giving

$$y = y(u_0),$$

where u_0 is the vector of assumptions made in the concrete case; here $u_0=(2,1)$.

5.2.3 What is conservatism in risk assessments? Discussion

From the set-up of Section 5.2.2, we are now ready to discuss what conservatism means in a risk context. The point of departure is the risk index y, which can be written

$$y = y(u_0),$$

where u_0 is the vector of assumptions made.

So, what does conservatism mean in this context? Three possible interpretations come quickly to mind:

I) $u_0 \geq u^*$, where u^* is the 'best estimate' ('best judgement') vector of u ('best estimate interpretation') and $\geq$ relates to all components of the vector, i.e. $u_{0i} \geq u_i^*$
II) $u_0 \geq u_T$, where u_T is the vector of the 'true' parameters of u ('true parameter comparison interpretation')
III) The analysts are confident that $u_0 \geq u_T$ ('true parameter comparison interpretation with confidence statement')

We will study these in more detail in the following, but first some comments on the terms 'true' and 'best estimates' used for defining these three polices. What do these terms mean?

When referring to a 'true' *parameter* in interpretations II and III, we have in mind two different types of parameters: observable quantities and parameters of a probability model. The two parameters referred to in Section 5.2.2 (u_1: the number of fatalities if the events A, B and C occur and u_2: the number of leakages in the period considered) are of the former type, observable quantities. An observable quantity expresses a state of the 'world', i.e. a quantity of the physical reality or nature, that is unknown at the time of the analysis but will, if the system being analysed is actually implemented, take some value in the future (this is the 'true' value) and possibly become known. The notion of an observable quantity should be interpreted as a potentially observable quantity, the point being that a true number exists and, if sufficient resources were made available, that number could be found (Aven 2012c, pp. 193–4).

To clarify the meaning of a parameter in a probability model, we follow Bjerga et al. (2014). A probability model is based on a set-up which is thought-constructed and refers to an infinite number of situations similar to the one under study. Let us focus on the quantity *number of leakages* as an illustration. In this modelling set-up, one can refer to a 'true' distribution G, describing the variation in this infinite population of similar systems. We write 'true' in quotes, as its meaning exists only within this thought-constructed set-up. As a model of this 'true' distribution, we may introduce the Poisson model, with parameter λ. Hence, the frequentist probability of at least one event in a period of length 1, is $p = 1 - e^{-\lambda}$. Now, by extension of this reasoning, we can talk of a 'true' value of the parameter λ, to be interpreted as the average number of events (leakages) in the infinite population of similar systems. Similarly, we may interpret p as the fraction of situations with at least one event in this infinite population. Here, G and λ (and p) are unknown and must be estimated. In a Bayesian study, focus is on the

epistemic uncertainties about this 'true' value of λ (expressed as prior and posterior distributions). In a traditional statistical analysis, one attempts to estimate the 'true' value of λ and give, for example, a confidence interval for it. For the sake of simplicity, it is common to say that one estimates λ and makes confidence intervals for λ.

In the following, when discussing II and III, we need to interpret the 'true' parameters u_T in this way. For knowledge-based probabilities, such 'true' values have no meaning. For the two examples studied in Section 5.3.2, 'true' parameter values can be defined for the frequentist probabilities r, p_1, p_2 and p_3, but not for the knowledge-based probabilities P(Y = 2), P(A), P(B|A), and P(C|A,B). In both examples, 'true' parameter values can be used for the observable quantities u_1 (the number of fatalities if the events A, B and C occur) and u_2 (the number of leakages in the period considered).

The 'best estimate' is the best judgement figure of the assessor, given the data, information and knowledge available, at the point of analysis, concerning the value of the unknown quantity of interest. It can thus always be determined. However, following a conservative policy as in I, the best estimate may not be specified – only the conservative value is needed. A main motivation for the conservatism is, as discussed in Section 5.2.1, to ensure that the system does not falsely satisfy an acceptance criterion (a threshold risk level). The choice of value is also a matter of resources – collecting more data/information and using additional computing efforts has a cost, and the conservative policy I could be seen as an attempt to reflect the level of resources used. An interval may be determined for an unknown quantity, for example the minimum and maximum number of people exposed to a type of accident scenario, and then the analyst often uses the conservative end of that interval.

The two policies I and II are fundamentally different, as seen from the above discussion. It may be questioned whether it is meaningful to also consider policy III applied to the best estimate, leading to a formulation like: 'The analysts are confident that $u_0 \geq u^*$' ('estimate comparison interpretation with confidence statement'). However, the best estimate can always be determined and, hence, uncertainties (and confidence statements) concerning $u_0 \geq u^*$ will not be an issue: we know that $u_0 \geq u^*$ by the way u_0 has been determined.

Best estimate interpretation I

In the example, the number of fatalities is assumed to be 2 if the events A, B and C occur. We have conservatism of type I if 2 is at least as large as the analyst's best estimate of this number, i.e. $2 \geq u_1^*$. The interpretation for assumption b is analogous. The interesting question now is how to

interpret the risk index y when this conservatism policy is adopted. As we have assumed that y is an increasing function in each u_i, it follows that the policy leads to a risk metric value that is larger than or equal to the best estimate. That is all that we can say. If the analysis presumes the existence of a 'true objective' risk value that we seek to estimate, the produced risk metric value y is thus more likely to be larger than this true value, compared to the best estimate – but, as for how much, we have no basis for making a judgement about that. If the metric is used for comparison with some tolerability or acceptance level and the derived risk metric is below this value, it is thus more likely that the true risk is also below this level than the best estimate. As such, the policy is conservative; see Figure 5.3.

A comment on the term 'true risk' is pertinent. The existence of such a value must not be confused with with the issue of 'true' parameter values as discussed above. The presumption that a 'true risk' exists is controversial – it is used for some risk perspectives, but it has no meaning in others; see Chapter 4 and Aven (2012a).

Returning to Figure 5.3, the reference is the acceptance or threshold level. There could still be a large probability that the true risk is above this level. Hence, the conservative policy is only to some extent able to reflect the uncertainties that are linked to the assumptions.

Under this policy, the risk metric is more robust for changes in the assumptions, in the sense that the risk metric y ($y=y(u)$) will be below the derived value $y(u_0)$ for all values of the parameters u below the specified assumption u_0. It is seen as likely that this set of u ($\{u: u \leq u_0\}$) covers the true assumption values u_T, as u_0 is larger than or equal to the best estimate. We have no basis for expressing how likely. Thus, the level of conservatism cannot be stated.

Adopting this policy, we can in addition say that it is more likely that worse outcomes will be the result than if the best judgements are adopted. As such, if a tolerability or acceptance level is used for a reference purpose, the produced risk metric has an element of conservatism in it. However, we cannot measure the degree of conservatism. These properties of the conservative approach also apply when the analysis is not based on the assumption that a true risk exists.

Next, we discuss the extent to which the conservatism policy leads to a change in the strength of background knowledge. To evaluate this, we need to clarify the purpose of the metric. Say first that we use it for comparison with this reference value (tolerability, acceptance criterion). Think about assumption a in our example; the number of fatalities is assumed to be 2 if the events A, B and C occur. Suppose the best estimate is 1. Has this change in u_1 increased or decreased the strength of knowledge on which the risk metric y is based?

If the risk metric is below the reference value, we can say that the strength of knowledge supporting the judgements is stronger, for the reasons discussed above, for example that the risk metric is more robust for changes in the assumptions. However, if the risk metric is above the reference value, the strength of knowledge is weakened. From a cautionary safety perspective, it may be argued that this weakening is less problematic than the strengthening of the knowledge in the 'below the reference value' case.

Now, suppose the purpose of the analysis is to compare the risk for two options. Then this conservative policy leads to a weakened strength of knowledge, as there is no way to evaluate the importance of the changes made. If, for example, the risk metric y in option 1 is higher than the corresponding risk metric for option 2, we cannot know whether this difference is simply due to the conservatism assumptions. Other conservatism assumptions could change the ranking. A comparison on the basis of best judgements u* is obviously more informative than policy I, using u_0 as the comparison does not depend on the arbitrariness in the effects of the conservative assumptions made.

True parameter comparison interpretation II

In the example, the number of fatalities is assumed to be 2 if the events A, B and C occur. We have conservatism of type II if 2 is at least as large as the true number of fatalities, i.e. $2 \geq u_{1T}$. We see quickly that this policy cannot be used in practice, as u_T is unknown in most cases. If it were known, we should of course use this value in the analysis. Often it refers to future quantities, as in examples a and b, and then they are obviously unknown, or they could be parameters of a probability model and then they are also

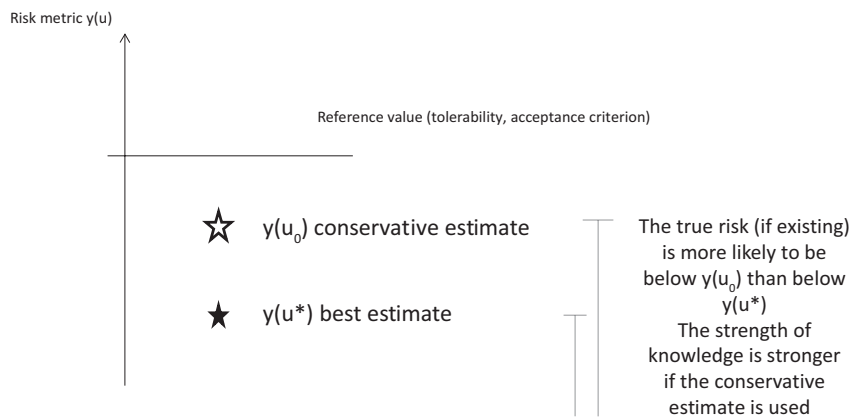


FIGURE 5.3 Illustration of the case when both the best estimate and the conservative estimate are below the reference value (based on Aven 2016d)

unknown in most cases. We see that we are led to policy III, as we need to reflect in some way about how sure or confident we are with respect to $2 \geq u_{1T}$ being the case.

True parameter comparison interpretation with confidence statement III

In the example, the number of fatalities is assumed to be 2 if events A, B and C occur. We have conservatism of type III if we are confident that 2 is at least as large as the true number of fatalities, i.e. $2 \geq u_T$. But what does being confident mean, and what are the implications for the risk metric and decision-making?

Being confident must mean that the analyst judges '$2 \geq u_T$' to be likely, but there is no indication of how likely. The natural interpretation of 'likely' is a knowledge-based probability, meaning that, if the analyst assigns a 0.90 probability for the event occurring, the uncertainty and degree of belief in this event occurring is judged the same as randomly drawing a red ball from an urn comprising ten balls where nine are red; see Section 3.1.1 (Lindley 2006, Aven 2012b).

An interpretation of being confident is thus that the analyst's knowledge-based probability for '$2 \geq u_T$' is large. We cannot specify one value, but, for most situations, a probability number in the order of 0.90 and higher would be considered large.

We may give a similar interpretation for assumption b. An important question is then how confident we are that both these events will occur. As an illustration, let us use 0.90 for each statement in isolation. Let us assume first that we judge the two events as independent. Then the probability that both events occur is $0.90 \times 0.90 = 0.81$, and we see immediately that, if the number of assumptions is high, the probability of all events occurring would be very small. The independence assumption could be an issue in many cases, yet the message would be the same: in the case of many assumptions, it would be difficult to conclude that we are confident that all assumptions are met.

There is one more complicating issue related to this policy. The probability assignments are based on background knowledge and this knowledge may be more or less strong. The analyst may have poor knowledge supporting the confidence statements, even if a high probability is assigned. Or, rephrased, the analyst may be sure that the statement is true, but the actual support for the judgement may be relatively poor. Seen from the decision-maker's point of view, this aspect is important, as surprises can occur relative to the beliefs and judgements made by the analyst.

Again, one can argue that there is a type of conservatism in this policy, but there is no way of expressing the magnitude of the conservatism. Let us look into the policy in relation to the two different uses of the risk metric.

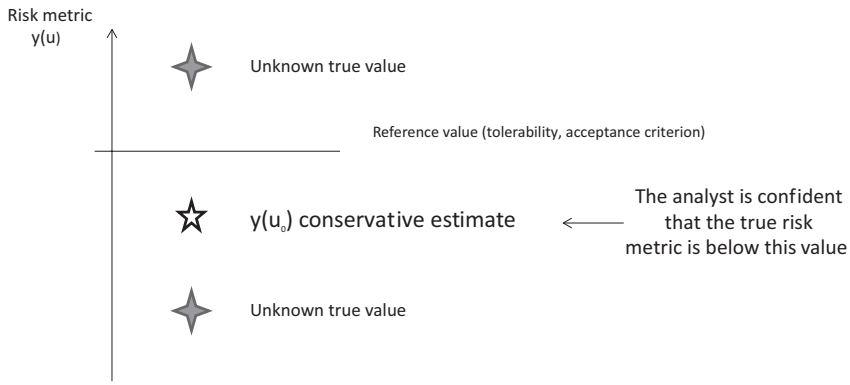


FIGURE 5.4 Illustration of the case when the analyst has established a conservative estimate, which is believed to be larger than the true risk metric value (based on Aven 2016d)

If the metric is used to compare the risk with some reference value, a derived risk metric below this value would provide an argument for the true risk metric (tacitly presuming its existence) also being below this value; see Figure 5.4. However, it is not clear how we should express any confidence related to this, as the approach does not allow for precise uncertainty statements. If the derived risk metric is above the reference value, a cautious safety policy would be to use the result to impose measures to reduce the risk, even though the true risk metric may not be above the reference value.

If the risk metric is used for comparing options, this conservative policy is problematic in the same way as policy I, as we do not know whether the difference found between the options is due to the conservatism assumptions. The decision-making could easily be misinformed because of the conservatism policy.

5.2.4 Discussion

A fundamental principle in risk management is the cautionary principle, which basically says that, in the case of risk and uncertainty, caution should be shown, for example by implementing risk-reducing measures or even avoiding the activity under consideration (see Section 7.3). It reflects a "better safe than sorry" policy (Viscusi et al. 1997). Conservatism in risk assessments can be viewed as a means to ensure such a policy. On an overall level, the policy seems attractive, using statements of the type "Conservatism involves a preference for erring on the side of overstating as opposed to understating risk under conditions of uncertainty" (Perhac 1996). The above analysis has shown that it is problematic in many ways. We have pointed to several issues.

First, the policy obstructs meaningful comparisons of options with respect to risk, one of the main purposes of risk assessments. If a difference between, for example, two design arrangements is derived or we are to measure the effect of a risk-reducing measure, we cannot know whether the difference is due to the conservatism in the assumptions or other factors. The policy leads to an analysis set-up that makes it impossible to use the risk assessment actively as a decision support tool for comparing solutions and measures.

Secondly, if the policy is used in relation to the acceptance or not of solutions and arrangements, by comparing the risk metric to some reference values (tolerability/acceptance criteria), there is no support from the policy on the magnitude of the conservatism. This makes it difficult to interpret and use the policy in practice. Of the three policies studied in the previous section, only the first one can be said to pass a basic scrutiny test. The second fails, as the true assumption values are unknown, and the third involves problematic statements of confidence linked to how likely the assigned conservative values are, relative to the true risk values. If the risk metric derived using conservative assumptions falls below the reference value, we cannot know whether the true risk metric is below it. And if the conservative risk metric is above the reference value, we may incorrectly conclude that the risk is too large and risk-reducing measures are required. Although the latter type of error could be consistent with the cautionary principle and a cautious safety thinking, the policy makes it difficult to conduct conscious judgements of when and to what extent such caution should be implemented. The costs of the measures needed to reduce the risk may be considerable, but the conservative risk assessment hampers the necessary cost-benefits type of evaluations, balancing the different concerns.

Policy I is general – it does not presume the existence of an underlying true objective risk to estimate – and it can thus also be used within a broader risk framework, as presented in Chapter 4. Using this policy for comparison with reference values, the risk metrics become more robust regarding changes in the assumptions, as explained in Section 5.2.3, in the sense that the risk metric $y(u)$ will be below the conservative value $y(u_0)$ for all u values below the specified assumption u_0. This is considered the main gain of using a conservative policy. Before concluding on the application of conservative policies in risk assessments, we need to reflect on what the alternatives are, as well as their pros and cons. A possible alternative to a conservative policy is to use best judgements and include sensitivity analysis and judgements on the strength of knowledge supporting the computations of the risk metrics. This means the specification of assumption values as exemplified above – intervals are not used. The sensitivity analysis reflects on the effects of using

lower or higher assumption values. Let us briefly outline the approach for the example considered in Section 5.2.2.

An alternative approach to a conservative policy

The alternative to a conservative policy, as discussed above, is to present the best judgements of the risk and the risk metrics and in some way reflect uncertainties and the strength of knowledge supporting the judgements made, in line with the ideas presented in this book. The example of Section 5.2.2 will be used to summarize some key features of this policy.

The point of departure is one or more risk metrics, as P(Y=2) and r* in the example. Consider first P(Y=2), where P refers to a knowledge-based probability. There is no uncertainty about this probability, as it expresses the analyst's uncertainty (and degree of belief) about the event 'Y=2'. However, the probability is conditional on background knowledge K – we should write P(Y=2|K) to show this – and the strength of this knowledge is of importance for how to understand and use this probability in the decision-making context. For example, if the strength of knowledge is poor, it is not meaningful to use the metric for direct comparisons with reference values and comparisons of options as discussed in the previous section. On the other hand, if the strength of knowledge is strong, such judgements have stronger justification. For some assessment methods for judging the strength of knowledge, see Sections 4.2 and 5.5.2. One of these methods addresses issues like the degree to which the assumptions made are reasonable/realistic, the degree to which data/information exist/s and are/is reliable/relevant, the degree to which there is disagreement among experts, and the degree to which the phenomena involved are understood and accurate models exist.

If the risk metric is r*, we focus on the estimate of an underlying presumed value (here, a frequency probability, but we may also think about cases where the quantity r is observable, such as the cost of a project). The point is that r is unknown and is estimated. In addition to the best estimate, uncertainty should be expressed, and this can be conducted in many ways, the two most common being:

- Assign a knowledge-based probability distribution of r
- Specify an uncertainty interval [a,b] such that $P(a \leq r \leq b) = 0.90$ or 0.95

In both cases, the strength of knowledge supporting the probabilities should be considered. And sensitivity analysis should be used to study how variation in assumptions and input quantities affects the risk metrics. Various importance measures can be used to identify the most critical assumptions

and quantities, see e.g. Borgonovo (2006) and Aven and Nøkland (2010), as well as Section 4.2.4.

5.2.5 Recommendations and conclusions

In this Section 5.2, we have looked more closely into the use of conservatism in risk assessments. This policy, which is based on replacing uncertain quantities with values that lead to a higher level of risk, is often applied to deal with uncertainties and lack of knowledge in risk assessment. An often-heard statement is "If the computed probabilities meet the pre-defined criteria with the conservative quantities, there is strong support for the 'real risk' to meet these criteria".

The analysis carried out above has shown that a conservative policy has severe shortcomings, and the conclusion of the analysis is that it should not be applied. The policy blocks the use of risk assessment as a tool for comparing options and studying the effects of potential risk-reducing measures, and, if it is used in relation to comparisons with risk tolerability and acceptance criteria, the policy provides no insights about the magnitude of conservatism, the consequence being that sound balancing judgements of benefits and costs cannot be meaningfully conducted. There are other approaches to conservatism that are much better in dealing with the uncertainties and lack of knowledge, as discussed in the previous section.

5.3 MODELS IN RISK ASSESSMENT: CAUSE–EFFECT RELATIONSHIPS

Risk assessments, and particularly quantitative risk assessments, are largely based on models to represent systems and processes. These models are conceptual constructs (typically translated into mathematical forms), built on a set of assumptions (hypotheses) on the systems and processes: for example, that the occurrence of an uncertain event of interest follows a Poisson distribution in time. The mathematical models include parameters, for example the (constant) rate of occurrence of the Poisson distribution: in practice, the values of these parameters are unknown and must be estimated on the basis of data and information available. The Poisson distribution is an example of a probability model which is commonly used in risk assessments to describe variation in unknown quantities characterizing the relevant system or process. It is discussed in Section 3.1.1 (item 5), Section 4.2.1 and Section 5.2.3.

Another model example is the event tree model y=f(x), discussed in Section 5.2.2. The model in this case takes the form $I(Y=2) = I(A) \cdot I(B) \cdot I(C)$, which is an example of a physical model (logical or event-oriented

physical model). An example of a 'quantity-oriented' physical model of the state of a system is $Y = X_1 - X_2$, where X_1 represents the capacity of the system and X_2 the load.

The modelling of a system or process needs to balance between two conflicting concerns: (i) accurate representation of the phenomena and mechanisms in the system or process and (ii) simplicity to allow the timely and efficient use of the model. Differences between the real-world quantities and the model outputs inevitably arise from the conflict between these two concerns.

5.3.1 Model uncertainty

We consider an event/system/process subject to a risk assessment and assume that, at the time of the assessment, no experimental data are available. Consider a quantity Z, whose true value is realized in the *future* and which we are interested in knowing. As an example, Z could be the actual number of fatalities due to a potential outbreak of a new virus. The actual value of Z cannot be known till after a potential outbreak. To predict the future value of Z, a model G(X) is developed. Both X and Z may be vectors. A simple model would be $G(X) = G(X_1, X_2) = X_1X_2$, where X_1 is the fatality rate and X_2 is the number of exposed people (say the number of citizens in a country). The predictions by G(X), then, depend on the structure G and the parameters X_1 and X_2.

Define:

Model error: The difference, $\Delta G(X)$, between the model prediction G(X) and the true future value Z, i.e. $\Delta G(X) = G(X) - Z$.

Model output uncertainty: Uncertainty about the magnitude of the model error.

Note that, according to this definition, model error and model output uncertainty are different, yet connected, concepts. The distance between the present time prediction G(X) and the future value Z is a well-defined quantity, referred to as the model error. As this model error cannot be known at the time of the prediction, we have uncertainty – model output uncertainty. Returning to the above virus example, say that prior to the outbreak of a virus the model G(X) predicts 50 fatalities. Then, after the outbreak is over, we count 33 fatalities caused by the virus. The derived distance, 50-33=17, would be the true model error. However, at the time of the prediction, we cannot know with certainty that the true model error is 17 – or any other value for that matter. We are facing model output uncertainty. This uncertainty is actually *epistemic* uncertainty about the size of the model error and,

hence, it may in theory be assessed using a suitable tool for measuring this type of uncertainty, like knowledge-based probabilities and imprecise probabilities, with related judgements of the strength of knowledge supporting these probabilities as discussed in Section 4.2; see also Bjerga et al. (2014).

Model output uncertainty results from two components:

Structural model uncertainty: The conditional uncertainty associated with the model error $\Delta_G(X)$, given the true value X_{True} (i.e. $\Delta_G(X_{True})$).

Input quantity (parameter) uncertainty: The uncertainty associated with the true value of the input quantity X.

The structural model uncertainty expresses the epistemic uncertainty under the condition that the input parameters are known (the true values). In other words, the structural model uncertainty expresses uncertainty about the model error when we can ignore uncertainty about the parameters X and relates then to the model structure G itself. Typically, this uncertainty is associated with assumptions and suppositions, approximations and simplifications made in the modelling. Input quantity (parameter) uncertainty, on the other hand, reflects epistemic uncertainties about the true value of X.

Sources of structural model uncertainty stem from actual 'gaps' in knowledge, which can take the form of poor understanding of phenomena that are known to occur in the system, as well as complete ignorance of other phenomena. This type of uncertainty can lead to 'erroneous' assumptions regarding the model structure. Other sources of structural model uncertainty stem from approximations and simplifications introduced in order to translate the conceptual models into tractable mathematical expressions.

The characteristic that no experimental data exist at the time of the assessment leads us away from classical statistical tools for the validation and subsequent accreditation of the model. Instead, validation transforms into the utilization of expert/analyst argumentation, based on established scientific theories and specific knowledge about the system, which the model assessed intends to describe.

Discussion

Model uncertainty has been thoroughly discussed in the literature; see Bibliographic Notes. Classic examples of such approaches are the alternate hypotheses and adjustment factor approaches (Zio and Apostolakis 1996). In the alternate hypotheses approach, a plausible set of models based on alternate hypotheses is used. These hypotheses are then assigned individual probabilities, reflecting the analyst's relative confidence in the truth of the alternate hypotheses. Differently, the adjustment-factor approach uses the

output of a single-best model, which is then adjusted by a multiplicative or additive factor to account for the uncertainty directly. Since this factor is in general unknown, probability distributions are introduced to provide a measure of confidence for different values of these factors. Another example is that of Rosqvist and Tuominen (2004a), which is based on a qualitative score assessment of direction of bias toward risk, where each modelling assumption is given a score: no bias, conservative or optimistic. For instance, if an assumption is deemed to represent the physical or social phenomena truthfully without any bias, then it is given the score 'no bias'.

The problem of model uncertainty is important for the accreditation of the model, for its use in practice. Accreditation is viewed here as reaching a required quality level of a model by validation, for its certified use. Clearly, this requires that model uncertainty be sufficiently small for confidence in the use of the outputs produced by the model. What is sufficiently small is of course dependent on the purpose for which the model is to be used. In practice, model accreditation stands on the evaluation of the comparison of the model predictions with the corresponding true values of the predicted quantities, for establishing the level of confidence in the model predictive capability needed for the intended use of the model.

In the case that experimental data are available, a wide range of statistical methods can be used for validation in order to accredit a model. These methods include both traditional statistical analysis and Bayesian procedures; see, for example, Bayarri et al. (2007), Jiang et al. (2009), Kennedy and O'Hagan (2001), Meeker and Escobar (1998), Xiong et al. (2009) and Zio (2006). However, these methods are not within the scope of the present analysis, in which situations with little data are available.

Model validation is often linked to model verification (and is often referred to as Verification and Validation, or simply "V&V"), which is commonly understood as the process of comparing the model with specified requirements (Knupp 2002, Oberkampf and Trucano 2002, Rebba et al. 2006, Roache 1998). The verification part is obviously important in many contexts to produce a model that meets the specifications.

Finally in this section, some words about the concept of 'completeness uncertainty'. This is thoroughly discussed in the literature and will be addressed in more detail in Section 5.4. It can be viewed as an aspect of model uncertainty (Bjerga et al. 2018) and relates to the discussion about potential surprises. Consider the following example.

Risk is described according to (A',C',Q,K), using the terminology introduced in Section 4.2. The concept of completeness uncertainty relates to the degree to which the set of events A' is complete, i.e. covers the actual A occurring. There could be many reasons why A' is not complete, for example that some events are ignored because they are considered extremely unlikely,

leading to a negligible risk contribution, or because they are unknown to the analysts. Clearly, this lack of completeness could contribute to model error G(X) – Z, as an event could occur which is not reflected in the model used. See Section 5.4 for further details.

5.3.2 Causality: Cause–effect relationships

A cause is a challenging concept. Philosophers have discussed it for many hundred years, at least since the days of David Hume (1711–76). In general, we can say that for B to cause A, at a minimum, B must precede A, the two must covary (vary together), and no competing explanation can better explain the correlation between A and B. The concept is used in many contexts of risk assessment, and in some of these the meaning is rather straightforward.

Think of a fault tree analysis of a top event A, which concludes that this event occurs if the event B occurs or the event C occurs. This means that a model is developed, and it states that B causes A to occur, and C causes A to occur. As an example, let A denote the event that a person, John, fails to produce a report on time. Here, B can be that John becomes sick and cannot work as planned and C that the production equipment fails, which delays the report. This is a simple example, showing how the events B and C cause the event A to occur. The analysis is a causality analysis. It can help John reduce the failure risk, by focusing on measures to reduce the probabilities of B and C occurring.

Fault trees, event trees and influence diagrams are often much more complicated than this example. However, the basic logic is the same: a model is developed which provides a set of events, whose joint occurrence leads to the occurrence of the top event A. As such, they cause A to occur. Figure 5.2 demonstrates a similar type of model, showing that an explosion scenario is caused by a hydrocarbon leakage, ignition and explosion.

Such a model can be more or less good in reflecting the real world, as are all models. As for a risk assessment, we can discuss the reliability and validity of a model; see Section 5.1. If we can test the model and use it to generate observations, we can think along the lines of Figure 5.1. However, for many cases, such testing is not possible, and the model can fail to capture important aspects of the world, depending on the knowledge supporting the model generation, as well as deliberate simplifications made to make the handling of the model practicable, as discussed in the previous section.

Often such cause models are extended by adding sets of risk influencing factors. It could, for example, be the level and quality of training and the level and quality of the maintenance work. In accident analysis, it is common to refer to the concept of ‘root causes’ (Cojazzi and Pinola 1994), which is based on the idea that it is possible to find a basic cause that is the root or

origin of the problem (Hollnagel 2004). Following such thinking, the 'root' cause could be identified as, for instance, 'poor quality of the maintenance work'. However, as discussed by, for example, Hollnagel (2004), the concept of root causes is not meaningful. There will always be a need to specify a set of conditions, states and events to explain an accident. It is not enough to point to one underlying factor. Rather, we can think of causes as aspects of the situation that are seen as necessary and sufficient conditions for the observed effect to have occurred (Hollnagel 2004). The cause is thus a construction, given the accident. However, it is always possible to think about these conditions, states and events using thought constructions acknowledging the limitations there will be in foreseeing all the various scenarios. For complex systems and activities, we know per definition that we will have problems in seeing all relevant conditions, states and events that possibly could lead to the accident. Surprises will occur.

Causality is a key concept in risk assessments and science in general. For example, science tells us that smoking is dangerous. The evidence is strong. There is basically no discussion about it. The scientific method has been used to prove that smoking has severe negative health effects. A number of statistical models have been established, linking lung cancer and smoking; see, for example, Flanders et al. (2003) and Yamaguchi et al. (2000). We also have strong phenomenological knowledge about why smoking is having these effects. The research provides knowledge about the health effects of smoking in the form of statements, such as "smoking is dangerous" and "smoking causes lung cancer", supported by statistical analysis. This analysis is concerned about two main issues:

a) What does it mean that smoking is dangerous? And that smoking causes lung cancer?
b) Uncertainty related to the correctness of these statements. How sure can we be that these statements are correct?

Issue a is commonly answered by referring to a suitable statistical and risk analysis framework. For example, a frequentist probability p may be introduced, expressing the fraction of persons belonging to a special population (for example, women of a specific age group) that get lung cancer. By comparing estimates of this probability for non-smokers and smokers and considering variations, for example related to the number of cigarettes per day and the duration of smoking, significant differences can be revealed, justifying the statements.

Hence, the statements can be interpreted as saying, for example, that smoking significantly increases the chances of getting lung cancer, where 'chance' is understood in a frequency manner. In this framework, uncertainty

is dealt with using concepts like variance and confidence intervals. Other frameworks exist, for example the Bayesian one, in which epistemic uncertainties of unknown quantities – such as p – are represented by subjective probabilities expressing degrees of beliefs.

For a specific person, this type of research cannot conclude. Its scope is populations or groups of people, not individuals.

The challenge is to separate causality from correlation. The statistical analysis may show that there is a correlation between two factors, but that does not prove causality. A classic example is related to a city's ice cream sales. These sales correlate with the rate of drownings in the city swimming pools, but there is no causality link between the two. The temperature (heat) may explain the correlation. The heat is an example of a hidden or unseen variable, also known as a confounding variable. There is considerable literature aimed at identifying spurious relationships, but it is difficult to eliminate them. It is easier to disprove causality – cause–effect relationships – than prove it (refer to Karl Popper's falsification theory). See textbooks in statistics and also Cox (2012), who discusses various aspects of causality in a risk analysis setting. As highlighted by Cox, there are many methods now available that can be used to study causality and, in particular, to analyse how changes are propagated through systems and how changes in the input lead to changes in the output.

5.4 RARE EVENTS

In risk assessment, we are typically faced with a huge number of potential scenarios and events; in practice, some of these are ignored, because they are either not identified or judged to be of low probability. However, a scenario or an event may occur, despite being extremely unlikely. Considering a large population of such scenarios and events, the occurrence probability is not necessarily negligible. In this section, we take a closer look at this challenge, the main aims being to clarify the issue and provide some recommendations on how to best handle it in practice. A main conclusion is that the risk assessment should be placed in a sufficiently broad framework, ensuring that the outcome and main event spaces are complete and sufficient focus is placed on the hypotheses and assumptions supporting the detailed scenarios that are identified.

5.4.1 What is the issue really about?

We are often surprised when a specific scenario occurs; we meet a person, John, on holiday, whom we have not seen for 20 years, or an accident occurs

where we experience a combination of conditions and events that is considered so unlikely. Think about the Deepwater Horizon accident. Here, this combination can be summarized as (NC 2011):

- Erroneous assessments of the results of pressure tests
- Failure to identify that the formation fluid penetrated the well, in spite of the fact that log data showed that this was the case
- The diverter system was unable to divert gas
- The cutting valve (blind shear ram (BSR)) in the blow out preventer (BOP) did not seal the well

If a judgement of this set of events had been made before the accident, an extremely low probability would have been assigned. Yet, it occurred. Is the explanation that this is just 'one out of a million' scenarios that could occur and that, before the accident, all these scenarios were possible? It may not be surprising that one of these scenarios occurs when we do not specify which of them. Aristotle (384–322 BC) pointed to this phenomenon more than 2,000 years ago, when stating "It is probable that improbable things *will* happen". As we know from probability calculus, the probability of a union of a set of disjoint events is the sum of the probabilities of these events. The occurrence of one event in a population may be quite likely, even if the probabilities for each event, seen separately, could be very low. If you selected a person you know before your holiday, it would not be probable that you would meet him or her, but if your event of consideration is any person you know, it may not be so unlikely that this event will actually occur.

A main task in risk assessment is to identify scenarios that may occur, and assess the risk related to their occurrence. The number of scenarios could be very large, and not all are considered for further analysis. Broadly, we can distinguish between the following categories of scenarios:

a) Not identified (an unknown unknown, i.e. a type of event that is not known; or an unknown known, i.e. an event type known by some but not by the analysts conducting this risk assessment).
b) An identified scenario and included in the risk assessment – its likelihood and risk are assessed, the scenario is followed up, and measures to meet it are discussed.
c) An identified scenario and included in the risk assessment – its likelihood and risk are assessed and found negligible. The scenario is not further studied.

But on what basis should we determine what is a negligible probability or risk related to a scenario? As discussed above for the Deepwater Horizon

and holiday examples, we need to be careful in removing scenarios on the basis of isolated risk and probability judgements. Very unlikely events may occur.

This section discusses this issue – ignoring scenarios in risk assessments. The topic has been addressed by many scholars, from Aristotle to researchers in statistics, quality management and risk assessments; see, for example, March and Shapira (1987), Klinke and Renn (2002) and Metzger (2010). Of special interest here is the concept 'completeness uncertainty', discussed in the probabilistic risk assessment (PRA) community and particularly in nuclear contexts; see Section 5.3.1. Completeness uncertainty relates to risk contributors that are not accounted for in the PRA model; it may be categorized as either being known, but not included in the PRA model, or unknown (NUREG 2013). Examples of sources of these types of incompleteness include the following (NUREG 2013):

- The scope of the PRA does not include some classes of initiating events, hazards, modes of operation or component failure modes.
- The level of analysis may have omitted phenomena, failure mechanisms or other factors because their relative contribution is believed to be negligible.
- Some phenomena or failure mechanisms may be omitted because their potential existence has not been recognized or no agreement exists on how a PRA should address certain effects such as the effects on risk resulting from ageing.

The following analysis seeks to bring new insights to the topic by:

- Reflecting on different types of formulations of scenarios and events. The more details are specified in a scenario, the more unlikely it is.
- The link between judgements of 'negligibility' and overall decision criteria and judgements. We see beyond the traditional criteria in the form of probability-based tolerability and acceptance criteria, to also take into account considerations of the strength of knowledge on which the probability judgements are based.
- Precision regarding what probability (likelihood) and risk mean in this context. Meaningful discussions of what are negligible probability and risk require that these concepts are clearly defined and interpreted.

We start by introducing a general set-up for explaining the problem of ignoring events and scenarios in risk assessment (analogous to the one studied in Section 5.2.2). A simple example is used to illustrate the ideas.

5.4.2 A formal set-up

We consider a future activity (interpreted in a wide sense to also cover events such as natural phenomena), for example the operation of a system, and focus on the consequences of this activity with respect to something that humans value. We may, for instance, have a special interest in a type of events that may occur, such as undesirable events linked to humans' health. Let A be the event occurring. In the oil and gas example presented in Section 5.2.1, A may, for example, be a major gas leakage leading to some fatalities. In the holiday example, A could be meeting our friend John.

In the risk assessment, we specify a set of events that we believe could occur. Let us call this set A' = {A_1',A_2', . . .}. The assessment may have a scope and restrict attention to some specific categories of events, for example only events that have the potential to lead to fatalities or events that are actually defined by the number of lost lives. The sets may, for example, be like this:

A' = {Uncontrolled discharges of hydrocarbons and fires, including process leaks, well incidents/shallow gas and riser leaks; structural integrity related incidents such as structural damage, and collisions; work accidents} (5.1)

A" = {0 fatalities, 1 fatality, 2 fatalities, 3 fatalities, . . .} (5.2)

In the holiday example, the sets could be:

A' = {John, Filip, Frank, Lisa, . . ., Jan} (5.3)

A" = {relatives, friends, colleagues, others} (5.4)

These two sets A' and A" are just two sets of events; no special meaning is attached to the superscripts ' and ".

We observe that the actual event occurring may or may not be captured by the specified sets of the risk assessment, A' and A". In the oil and gas example, A", defined by formula (5.2), would necessarily include the actual fatality number, but A', defined by (5.1), could lack some events, for example a loss of life due to some heavy storms (man overboard). In the holiday example, we have a similar situation, as the name identified may not cover the actual one met, but, using the categorization A" (formula (5.4)), all possibilities are necessarily covered.

The use of A' leads to incompleteness, as the specified values are to be considered a model of real life, and this model has limitations. In the coming discussion, models will play an important role, with their link between

output quantities (events) and input quantities (events) that together generate more or less detailed scenarios.

Let y denote a risk description (metric) used in the risk assessment (for example, the set of events A' and A" with associated assigned probabilities), and let x be a vector of parameters of the total model f used for deriving y. Hence, we can write

$$y = f(x). \tag{5.5}$$

As an illustration, consider the example in Figure 5.2, Section 5.2.2, linked to the oil and gas case. The model provides a link between the event "gas leakage" (A_1') and the number of fatalities (Z and A"). There is a potential difference between what the model expresses and what the actual quantities and events would have been, had the activity been realized; we refer to this difference as the model error. As discussed in Section 5.2.2, it is possible to analyse the system based on both knowledge-based probabilities and frequentist probabilities. In both cases, the model used is of the form $y=f(x) = x_1 \cdot x_2 \cdot x_3$.

In the risk analysis, we would typically have a number of such initiating events and trees, representing different types of events, as well as different areas where the events (for example, the leaks) could occur.

From this set-up and example, we are ready to discuss the issue of ignoring events and scenarios, by concentrating on two main types of decision-making situations. In the first, the risk assessment is to verify that the risk metric used meets some pre-defined criterion or limit, while, in the second, it is used to compare options with respect to risk, including studying the effect of implementing risk-reducing measures.

5.4.3 What does ignoring events and scenarios mean? Discussion

The point of departure is a risk metric y, computed by formula (5.5), $y = f(x)$, and a set of events/scenarios A', forming the basis of this metric. The actual event/scenario occurring is denoted A.

In relation to A', we have two main challenges:

(i) The analysis set-up excludes some events/scenarios B' from the set A' studied, as a result of unknown unknowns (a) and unknown knowns (b)
(ii) Some events/scenarios B' are excluded from A' and further analysis, due to judged low probability.

We study these in more detail in the following. In the oil and gas example, we noticed that A' did not include heavy storms and, in the holiday example, the

list of names was not necessarily complete. In addition, the analysis may have a scope that specifically addresses some events and excludes all others.

In theory, there is always a possibility of an unknown unknown, but if the phenomena are 'well understood', such events would be rare. The unknown unknowns represent risk, but this risk contribution is not added to the risk metric used. Per definition, there is no way of explicitly incorporating this risk contribution at this point in time; hence, the risk description needs to be understood as conditional on no such event occurring. For the John holiday example, this type of surprise is not relevant, and it is not considered a major concern in the oil and gas example, as the phenomena studied are rather well understood. For complex systems, however, the concept of 'well understood' is more problematic. Also, many petroleum activities need to be classified as complex; hence, care must be shown on this point.

The category (b) of unknown knowns is much more challenging. The analysts may overlook some events from the analysis because they are not aware of them. In the holiday example, John may overlook, for example, some people that he met on a journey some years ago. There are obviously many possibilities that the list A' is not complete, if defined before the holiday. In the oil and gas example, the list of A' events may also exclude some potential loss of life events when restricting attention to A' = {Uncontrolled discharges of hydrocarbons and fires; structural integrity related incidents; work accidents} defined by formula (5.1), as we noticed in Section 5.4.2, but this is easily rectified, so that the set should not allow for unknown unknowns and unknown knowns at this level of detail. For an industry with many years of experience, it is hard to think of ways in which people are killed on an offshore installation that are not covered by historical observations, with such a macro description level. If we add a category of 'others', all types of events are of course covered.

Detailed scenarios

Now, let us move to the more detailed scenario level. Here, surprising scenarios may occur. An illustrative example is the Heimdal incident in 2012 (PSA-N 2012).

Here, a hydrocarbon leak with a large leak rate occurred on the Norwegian continental shelf, in connection with the testing of two emergency shutdown valves (ESDVs). In preparation for testing of the valves, a pipeline was to be depressurized to flare. In the pipeline, a ball valve with a pressure of 16 bar was installed as the last barrier against the flare. This ball valve was in the closed position and was exposed to a pressure of 129 bar. The pressure caused the failure of the gasket flange to the valve and a consecutive gas leak estimated at 3500 kg with an initial leak rate of 16.9 kg/s. Gas was detected in a large area of the installation.

Prior to the incidents, the operating team was basing its risk scenarios on an understanding that the pipe was in accordance with current design practice, as then all the relevant pipe sections, even past the valve to the flare, would have withstood the process pressure. Hence, the order in which the three valves were opened would not be safety-critical. The relevant pipe section was, however, designed according to an older design practice, in which spec break (change of pipeline specifications) to a lower pressure class is upstream of the last valve to the flare. With such a design, the order in which the three valves are operated is safety-critical: if the last valve to the flare is opened last, the pipe will be subjected to higher pressure than designed for.

This knowledge was known to others in the organization, so the scenario that occurred did not come as a surprise to them – only to the operating team. Scenarios capturing this knowledge were not included in the analysis.

Events ignored due to low probability (ii)

Alternatively, these events could be seen as excluded, due to arguments in line with category (ii), ignored as being so unlikely. Theoretically, a number of scenarios may occur, but in practice simplifications are made and some events are ignored. This practice is of special interest for the present discussion.

Heimdal example and event tree model

In the Heimdal case, the operating team was confident that the system was a standard system and did not elaborate on related scenarios. The risk was concealed in the assumption made: the system is standard. Similarly, the analysts excluded the possibilities that more than two fatalities could occur in relation to the scenarios described by the event tree model shown in Figure 5.2. A number of possible scenarios are obviously ignored by this type of modelling. The argument would be that the probability and risk are so small that we can ignore them. The question we will discuss below is: can this be justified? And what are the 'risks' involved in doing so?

To simplify, assume in Figure 5.2 that we allow for three fatalities as the maximum number in the case that A, B and C occur. Say the analysis has derived a probability of two fatalities associated with this tree, equal to 2×10^{-5}, and the analysts judge the probability of three fatalities to be a lower order of magnitude: hence, about 2×10^{-6}. With a number of trees, the probability of three fatalities could be much larger but may still be considered so low in relation to two fatalities that it is not included in the analysis. To support the decision-making, the risk contribution from three fatalities is not considered essential.

Similar arguments could be used for four, five, . . . fatalities. The probabilities become very low on the basis of the calculation of the model.

The possibility of a large number of fatalities could be summarized by a probability of say ten fatalities equal to 2×10^{-7}. For the purpose of the risk analysis, this contribution could be found to be of minor interest, when comparing the relevant decision alternatives or comparing the risk numbers with some pre-defined risk acceptance criteria (such as the Fatal Accident Rate, the expected number of fatalities per 100 million exposed hours). It may not be ignored completely in the analysis but, as the probability is judged to be so low, this risk contribution is not given the same attention as the risk linked to one and two fatalities.

The probability judgements are based on a background knowledge K, which captures assumptions, more or less tacitly formulated, as in the Heimdal case. The low probability numbers assigned for extreme scenarios are conditional on the belief that the system is a standard one. However, the system was a special one. The idea that it was special may not have been an issue at all but, if it had been, the probability that the system was special could have been judged as so low that it would not be believed to be a problem. Another case from the oil and gas industry illustrates this point.

Ula example

On 9 December 2012, there was a large hydrocarbon leak on the Ula production platform (PSA-N 2013). The platform was in normal operation when the leak occurred. The direct cause of the leak was a fracture of the bolts that held together a valve in the outlet of the separator. Because of sweating in the valve, the bolts were exposed to produced water with a high content of chlorides and a temperature of 120°C. This resulted in chlorine-induced corrosion, which weakened the bolts, so that they eventually broke.

Sweating outside the valve was discovered on 29 March 2012. A risk assessment was conducted, and it was concluded that the valve could be replaced during the maintenance shutdown in the summer of 2013. A prerequisite for the choice of material in the valve bolts is that they do not come into contact with the medium (produced water). When sweating in the valve was discovered, this assumption was not followed up in the organization.

There had previously been similar corrosion problems on Ula, and the issue of corrosion due to produced water was known to the operator. The experience associated with sweating was not used in the assessment of the specific sweating problem on Ula.

In this case, the operating team considered the probability of a problem occurring – leading to fatalities – to be negligible. As for the Heimdal case, the event can also be placed in category (i), but it is clear that, when the operating team accepted the risk linked to deferring the replacement, the likelihood of a serious scenario occurring due to this sweating issue was considered negligible. The likelihood and conclusion were based on poor background knowledge, an assumption that did not hold.

Let K_1 denote the background knowledge of the analysis team, which includes a belief (assumption H) that the system was a standard one in the Heimdal case and that the valve sweating was not a problem in the Ula case. With this background knowledge, the operating teams do not consider scenarios with extreme outcomes in conflict with K_1 and H. Such scenarios are not thought of or they are ignored because the judged probabilities for the set of such scenarios are negligible: $P(\text{the set of such scenarios} | K_1, H) \approx 0$.

We see from this analysis that events are ignored in risk assessments and that this may have critical consequences for the decision-making. Now, we will discuss how we can meet this challenge and see if there are possibilities to improve current risk analysis practice.

5.4.4 Recommended approach: How to improve the foundation and practice of risk assessment

Let us first consider the John holiday example. This example is very simple, and it is easy to see how we should proceed to ensure that we carry out a proper treatment of the various events/scenarios. First, we need to specify an outcome space that is sufficiently wide to cover all potential people that John can meet. This can be done in different ways, by grouping them into categories like formula (5.4):

A" = {relatives, friends, colleagues, others}

and then specifying all the names one is able to identify within each category. The category "other" must also be used for the sub-categories, relatives, friends and colleagues. Then the assessment of uncertainty can start. Probability is the common tool, but it needs to be supplemented by judgement of the background knowledge on which the judgements are based.

Take two cases: one in which a very crude analysis of possible names is listed and one in which a very detailed, thorough analysis is carried out with a systematic review of 'everything' John has done in his life. We would expect, then, that the list in the latter case includes many more names and the 'other' categories are nearly empty. Let us say that the numbers of names identified in the two cases are 100 and 1,000, respectively. We use these names as models of the situation considered but add 100 in the former case to take into account non-identified persons. Using the numbers 200 and 1,000, John can make an assignment of the probability of meeting one of these people during his holiday. He takes into account many factors, for example known numbers of how many people from his country visit this country in a year and the fact that this is one of the peak weeks for travel to this place. Let us say that he comes up with the (interval) probabilities 1–5 per cent and 5–25 per cent, respectively. Clearly, the background knowledge

in the latter case is stronger than in the former case, and the numbers can be given more "weight". Hence, meeting somebody John knows on this holiday cannot really be considered surprising, as he would judge the probability to meet one person he knows – without specifying his or her name in advance – to be quite likely.

Oil and gas example

Now let us return to the oil and gas example. To formalize the discussion, we make a distinction between the outcomes (for example, expressed as the number of fatalities), hazardous events (for example, hydrocarbon leakages), and risk sources that can lead to these events and outcomes. As in the John example, it is essential to ensure that the outcome space covers all potential outcomes. If the number of fatalities is the quantity of interest, this is straightforward: the set must cover {0,1,2, . . .}, or {0,1,2, . . ., M} if it is known that the maximum number of fatalities is bounded by M. In the analysis in Section 5.3.2, based on the event tree of Figure 5.2, the number of fatalities was restricted to two. There may be reasons for this – there could be a maximum of two people exposed – but if this is not the case, it is important to have an initial model set-up that does not exclude unlikely events. It may be judged unlikely – at the design of the model – that more than two people are killed, but further analysis may challenge this judgement. The rule should, therefore, be to always frame the assessment in a way that includes all possible outcomes, using, if necessary, categories of 'others' to stimulate thinking that goes beyond the defined outcome categories. This relates to a fundamental idea in risk analysis (the so-called backward approach – Aven 2015e), where the point of departure is the outcome of interest (here, say at least three fatalities), and we ask what kind of events and risk sources can lead to such an outcome.

Using the event tree model, the key element of the analysis is the identification of the events, the leakage, the structural collapse, etc.

Again, the recommendation is to initially include a complete set of events, 'complete' of course seen relative to the purpose of the analysis. An example could be

> A" = {Uncontrolled discharges of hydrocarbons and fires; structural integrity related incidents; work accidents; others}.

For the oil and gas industry, it should be possible to develop a complete list of events at this level of detail, avoiding unknown knowns, so the 'others' category is reduced to unknown unknowns. In the John holiday example, John may easily leave out some names from the list because he has forgotten them: an event which can be classified to be of the unknown known type.

Risk sources

Then, we come to the risk sources, the types of situations and the sources for events to occur. This element is more difficult to define, as it covers so many different aspects. One example is a pipe section of hydrocarbons with flanges and valves, which has the potential to give rise to a leak. Another example is a maintenance activity on a valve, which also has the potential to cause a leak. In a fault tree, we develop sets of basic events which can lead to the top event, and we refer to this as a cause analysis – identifying sets of basic events that cause (lead to, explain) the top event. A fault tree is to be seen as a model of the real system and does not capture underlying factors linked to, for example, management and organizational issues, such as the importance of training. However, such factors are often modelled using influence diagrams – Bayesian belief networks; see for example Ayyub (2014) and Meyer and Reniers (2013). The models are crude representations of the many factors that can lead to a hazardous event, and often the justification of the models is rather poor, as there is no well-established theory supporting the modelling. The number of factors that can be combined to generate the event could in theory be huge but, to make a reasonable model of the system, only a limited number is selected. Yet, the modelling can be useful, for example, in studying the effect of such factors on risk and seeing how various measures based on these factors influence the risk.

In a risk assessment, the degree to which the risk sources (causes, explanations) are in fact modelled varies, but, for practical risk management, in particular in the operational phase, they are the key to ensuring safe activities, as the risk is 'rooted' in these sources and the risk-reducing measures to a large extent need to be based on these sources. However, the complex links between the sources, on the one hand, and the events and outcomes, on the other, represent a big challenge for the risk management, whether or not models of the phenomena are developed. Hypotheses and assumptions, more or less strongly justified, in reality often form the basis for the decision-making. The Ula and Heimdal cases mentioned in Section 5.3.3 provide two illustrating examples: in the Heimdal case, the thesis was that the system was a standard one, whereas, in the Ula case, it was the belief that the valve sweating was not a problem.

A huge number of scenarios – linking risk sources with the events and outcomes – can be generated, but the hypotheses and assumptions exclude many or most of them. What is considered is often a limited set of thinkable scenarios, based on the risk assessment carried out and the basic beliefs that the relevant personnel have on the issue addressed.

Scenarios are here excluded from further analysis and decision-making, as they are not known to the operating team (unknown knowns) and because

the likelihood is judged to be so small that the scenarios are not believed to occur. For the latter category, we again need to question whether neglecting scenarios due to low likelihood can be justified, as there are so many potential scenarios.

Seeing the link between sources, events and outcomes as a complex system, we would not be able to identify all scenarios of interest – the actual scenario occurring will come as a surprise (Turner and Pidgeon 1997). The key for the analysis and management related to such scenarios is to acknowledge that not all scenarios will be identified – they can be viewed as unknown knowns, and some that are identified but not believed to occur due to judged low probability can in fact occur, as there are so many of them and the judgements can be based on more or less valid hypotheses and assumptions.

Methods for identifying and analysing the risk sources and their link to events and outcomes (the key elements of the so-called bow-tie), can improve the insights into the system, but it is critical to acknowledge that the judgements made can never fully capture all risk aspects, for the reasons discussed above. Hence, we need to look for ways to think outside the normal box, challenging the hypotheses and assumptions on which the events and scenarios are built. It is beyond the scope of the discussion here to describe methods that can be used for this purpose; see Aven (2014b) for some selected approaches and methods, covering inter alia analysis methods to identify events/scenarios, such as the anticipatory failure determination (AFD) method of Kaplan et al. (1999) and red teaming, which serves as a devil's advocate, offering alternative interpretations and challenging established thinking (Masys 2012), see also Section 8.3. In addition, it is essential to be able to read signals and warnings – we must avoid missing or ignoring important early signals and precursors of serious events (but also, of course, avoid exaggerating them). The focus on signals and precursors of serious events is a common feature of most approaches that seek to meet surprises and the unforeseen. If we look at basic insights from organizational theory and learning, this feature is a main building block. A good example is the concept of collective mindfulness, linked to High Reliability Organizations (HROs); one of its five principles is sensitivity to operations, meaning a focus on reading the landscape and taking adequate actions.

In the handling of unknown known scenarios, there is a vast body of literature on methodology, covering *how to* involve expertise (those that may know) in the analysis and decision processes, which is relevant here. Special reference is made to the quality management area with its focus groups, affinity diagrams, etc. (e.g. Sower 2014). See also Veland and Aven (2015), who present an adjusted job safety analysis with the intention of better addressing this type of risk.

5.4.5 Conclusions

A key task of risk assessment is to identify events and scenarios that can lead to some specified outcomes. Depending on how these are defined, the list of such scenarios and events can be more or less complete in the sense of capturing the actual one occurring. Hence, there could be risk contributors not captured by the analysis. To meet this risk, two main messages are drawn from the analysis in the previous sections. First, it is essential to define a set-up for the analysis that is sufficiently broad on outcomes so that all relevant types are covered. The use of a category 'other' may be necessary in some cases to ensure this, stimulating questions about how to obtain such an outcome.

We should aim at a similar thinking for the main events, where we need to have a special focus on unknown knowns. Unknown unknowns should also be covered but would normally be given less attention than the unknown knowns, as the latter category is much more likely to occur in most cases. Events at this level should not be excluded due to low probability.

For the risk sources with links to the events and outcomes, many scenarios will not be identified, or they will be ignored due to judged low probability. Care must be shown in this process, as the judgements on this part are so strongly based on hypotheses and assumptions which are often difficult to justify. The actual occurrence of the scenarios will typically come as a surprise relative to the existing beliefs, but it should be noted that, from a broader perspective – having insights about the correctness of these hypotheses and assumptions – the probability for any such scenario could be quite large. This means incentives to scrutinize the probability judgements made, with their background knowledge, using methods as discussed in the previous section. Any model and analysis of the source part needs to be seen in relation to the assumptions on which they are based. The risk assessments can improve on this area, as indicated in Section 5.4.4, but, for complex systems, they cannot predict with accuracy all scenarios that will occur. Hence, the appropriate management regime to meet the risk related to the operation of such a system must always combine risk analysis methods with measures of robustness and resilience, to cope with scenarios and events not identified or planned for; see Section 7.1. This is also the basic pillar for safety regulations in industry, but it is frequently challenged as being irrational and not placing sufficient weight on the real matters (Aven 2011c).

5.5 DIFFERENT ACTORS

In its general form, risk is *quantitatively* described by identifying a set of consequences C' of an activity and using a quantitative measure Q to express

the uncertainties related to these consequences. This risk description (C',Q) is based on a background knowledge K, including assumptions on which the (C',Q) assessment is founded; refer to Section 4.2. As argued for in Section 4.2, it is essential to incorporate K and judgements of its strength in the risk characterizations. The purpose of the present section is to discuss in more detail the difference in perspective between the analysts, the decision-maker, and other potential stakeholders. Ways of characterizing the risk for the different actors are presented and discussed.

5.5.1 What is the issue really about?

It is common, at least in the engineering environment, to define risk by the consequences C' of the activity studied and the associated probabilities P (Ale 2002, Aven 2012a). We write Risk = (C',P), or (A',C',P), if we would like to highlight the events A' leading to some effects C'. Many variants of this definition exist, including the Kaplan and Garrick (1981) definition, where risk is equal to the set of triplets (s_i, p_i, c_i), where s_i is the *i*th scenario, p_i is the probability of that scenario, and c_i is the consequence of the *i*th scenario, i =1, 2, . . . N. The definition can be extended by replacing P with a general measure of uncertainty Q. Hence, risk is expressed by (C',Q) or (A',C',Q).

In risk assessments, the risk analysts present risk by showing (C',P) or (C',Q), using some suitable risk metrics and characterizations based on C',P and Q, for example expected losses, probability distributions for specific losses, risk matrices, etc. The risk metrics are often used as direct input to decision-making; for example, if the computed probability of a specific type of accident events is below a pre-defined criterion, risk is considered tolerable or acceptable. Risk analysts are of course aware of these metrics' dependencies on key assumptions made in the analysis, but these dependencies are not always communicated, the result being a rather mechanical use of the risk assessment and the associated criteria (Aven and Vinnem 2007). Not being experts on risk assessments, the decision-makers may expect a clear message from the risk assessment in the form of conclusive statements about, for example, risk acceptability or tolerability. Stressing the importance of the background knowledge and the assumptions for the risk metrics would easily confuse the decision-makers. The implication is that risk analysts may be tempted to downplay the results' dependencies on the background knowledge and the assumptions made.

For the risk analyst, risk is then expressed by (C',Q) (and related metrics) and is conditional on K, the background knowledge of the analysts. We write

Analysts' quantitative risk description: (C',Q|K). (5.6)

But can risk seen from the decision-makers' perspective be conditional on K? Should it not be unconditional, as deviations from assumptions made also represent risk that could be important for the decision to be made? We may have two situations, with identical assigned probabilities, $P(A|K_1) = P(A|K_2)$, but in one case the strength of the knowledge is strong and in the other case it is weak. The probability number itself does not reveal this aspect, but should not the risk description in some sense reflect this difference?

Yes, it should, as discussed in previous chapters (see e.g. Section 4.2). For the decision-makers, (C',Q|K) needs to be replaced by the unconditional triplet (C',Q,K_D), where K_D is a judgement of the knowledge K. This is in line with the recommendations made in Section 4.2.2, which expresses that in general risk should be characterized as (C',Q,K), where Q also include qualitative strength of knowledge judgements. The following analysis provides reflections and guidelines for how to define and perform the judgements K_D. The discussion is highly relevant for practical risk assessment and management, as will be shown by a simple example. The discussion seeks to add new insight, by clarifying the differences in perspectives between the analysts and the decision-makers (managers) and by providing insights on how to carry out the judgements of the background knowledge, to adequately support the decision-making.

Note that the decision-maker may have a good overview of the general competence level of the analysts but not detailed information about the strength of knowledge that the specific uncertainty (probability) judgements used in the risk assessment are based on. It is this knowledge we refer to here.

The discussion focuses on cases where we have a single decision-maker, like those we find, for example, in industry and business. However, the discussion and ideas are also applicable to situations with several decision-makers, who can have divergent preferences. The key issue is how to represent and characterize the risk results to adequately inform the decision-maker(s).

5.5.2 Example

The example is the oil leak case studied in Section 4.2.4. The risk was assessed pre the event and found to be negligible, yet the incident occurred.

A Safety Job Analysis (SJA) group meeting was arranged on the installation, as part of the preparation for this modification job. Guidelines exist for performing the SJA, which recommend, among other things, performing assessments of the identified hazards related to the different steps of the operation, using a risk matrix and specifying scores of the likelihood and the severity (consequence) of the hazard. The purpose of this assessment is to clarify the need for measures and to prioritize the actions to be taken. For the purpose of the present discussion, we assume that an SJA was performed in line with these guidelines, and we make a thought construction, assuming

that we are able to go back in time and add considerations, taking into account the knowledge dimension, as presented in the following.

Describing risk

Following the risk description terminology of Section 4.2, we define:

> A': the hot tap machine does not work according to design, resulting in an unintentional opening between the pipe and the passageway shaft,
>
> C': oil leak inside the passageway shaft, with related effects

A key aspect of the background knowledge K of the analysts is the assumption that there is reduced pressure inside the pipe system and hardly any evaporation will occur from the medium inside the pipe (stabilized oil).

The result is shown in Figure 5.5, using a standard risk matrix. Based on this background knowledge, the analysis team decides to place the scenario in the low probability and low consequence area of the risk matrix.

Thus, risk is described by a combination of the consequences C' and the probability P of the event A', given the background knowledge K, i.e. (C',Q|K). It is a description of risk seen through the eyes of the assessors.

Now, let us take the perspective of the operation management of the installation, or the top management of the company, who are not directly involved in the assessment of the risk. These units are responsible for the risk management and are concerned about what the actual consequences will be; they acknowledge that the risk descriptions used as input to the decision-making have limitations and are conditional on K. In the example, the decision-maker could also be a part of the analysis team in some cases, but let us assume in the following that we are in the common situation where the management and decision-maker are not directly involved in the generation of the risk description. For the sake of simplicity, say we have only two levels, the analysts and the decision-maker (management). The analyst team conducts the risk assessment and concludes that the risk is very small and the

Probability	*High*			
	Medium			
	Small	○		
		Small	*Medium*	*Large*
	Consequences			

FIGURE 5.5 Consequence and probability score of oil-leak scenario (based on Aven 2016c)

operation can be carried out without the implementation of special measures. The final go-ahead must be approved by the decision-maker – the managers. The question is then: what, for them, is an adequate risk description?

For the decision-maker and manager, it is essential to think first risk and not immediately the risk description produced by the analysts. For them, risk is (C,U), where C is the future consequences of the activity and U is uncertainty: not knowing what the consequences C will be. They have to acknowledge that the analysts have made a choice of which metrics to look at, what measure Q is to be used to describe the uncertainties, and that these metrics and the measure Q are based on some background knowledge K that may, to a varying degree, be strong or weak.

Relevant questions for the decision-maker and manager to ask would be:

a) How would the analyst team judge their own strength of knowledge?
b) How would other experts (or more generally stakeholders) judge the strength of the knowledge K?
c) How would they themselves judge the strength of the knowledge K, also taking into account the judgements made in a and b?

Based on these questions, we can formulate the following extended risk descriptions from the perspective of the decision-maker and manager:

a) Risk description for decision-maker and manager: (C',Q,K_S,K), where K_S is the analyst team's own judgement of the strength of their knowledge K.
b) Risk description for decision-maker and manager: (C',Q,K_{S1},K), where K_{S1} is the other experts' (stakeholders') judgement of the strength of the knowledge K.
c) Risk description for decision-maker and manager: (C',Q,K_S,K_{S1},K_D,K), where K_D is the decision-maker's (manager's) judgement of the strength of the knowledge K, also reflecting K_S and K_{S1}.

In theory, we may have more than one group of other experts but, to simplify, in the following analysis, we allow for a maximum of one. The challenge now is to develop suitable ways of conducting the strength-of-knowledge judgements, K_S, K_{S1} and K_D. For the decision-maker, there is a need to also address other quality features of the risk assessment and its use; see below. First, we look at K_S.

The analyst team's own judgement of the strength of the knowledge K

The analyst team needs to evaluate factors like (refer to Section 4.2.2): the reasonability of the assumptions made; the amount and relevancy of

data/information; the degree of agreement among experts; the degree to which the phenomena involved are understood and accurate models exist; and the degree to which the knowledge K has been thoroughly examined.

Various score systems can be developed on such evaluations. The following is based on Flage and Aven (2009) and Aven and Flage (2018).

The knowledge K is judged as weak if one or more of the following conditions are true:

w1) The assumptions made represent strong simplifications.
w2) Data/information are/is non-existent or highly unreliable/irrelevant.
w3) There is strong disagreement among experts.
w4) The phenomena involved are poorly understood; models are non-existent or known/believed to give poor predictions.
w5) The knowledge K has not been examined (for example, with respect to unknown knowns).

If, on the other hand, all (whenever they are relevant) of the following conditions are met, the knowledge is considered strong:

s1) The assumptions made are seen as very reasonable.
s2) Large amounts of reliable and relevant data/information are available.
s3) There is broad agreement among experts.
s4) The phenomena involved are well understood; the models used are known to give predictions with the required accuracy.
s5) The knowledge K has been thoroughly examined.

Cases in between are classified as medium strength of knowledge. To obtain a wider strong knowledge category, the requirement that all of the criteria s1–s5 need to be fulfilled (whenever they are relevant) could, for example, be replaced by a criterion expressing that at least one (or two, three or four) of the criteria s1–s5 need to be fulfilled, while, at the same time, none of the criteria w1–w5 are fulfilled.

A simplified version of these criteria can be obtained by applying the same score for strong but assigning the medium and weak scores when a suitable number of conditions are not met, for example, medium score if one or two of the conditions s1–s5 are not met and weak score otherwise, i.e. when three, four or five of the conditions are not met.

The strength is illustrated in the risk matrix by coloured events: dark, grey or white – alternatively red, yellow or green – depending on whether the background knowledge is considered to be weak, medium or strong, respectively. In our leakage example, we assume that an assessment of the strength of the knowledge was performed as described above and the result was as shown in Figure 5.6. During the assessment, the analysts identify

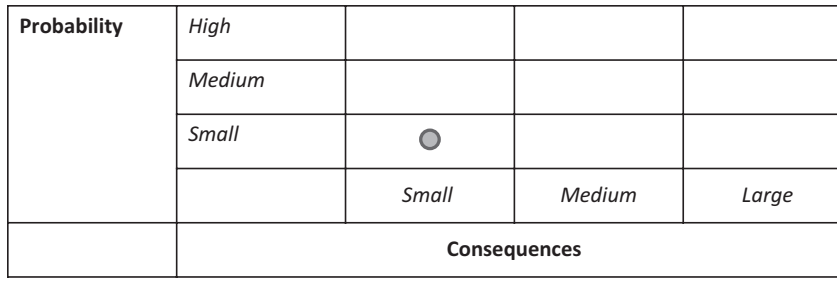


FIGURE 5.6 Consequences, probability and strength of background knowledge for the leakage example, reflecting the unclarified assumption (based on Aven 2016c)

an unclarified assumption: that the pressure inside the pipe reduces during the work. The group evaluates the above criterion and decides to assign a medium (grey) score for the strength of the background knowledge.

The above analysis relates to a specific probability assignment. The above assessment system for measuring the strength of knowledge can also be used for the total risk assessment being performed. As an input to the evaluation of the total risk assessment, a number of quality aspects can be considered; see, for example, the reliability and quality concepts discussed below and the criteria defined by Ford et al. (2008).

An alternative approach is presented in Section 4.2.2 for assessing the strength of knowledge of K, by looking into the risk associated with deviations from the assumptions made (Aven 2013e).

The other experts' (stakeholders') judgement of the strength of the knowledge K

This group may have different roles, depending on the situation. The group may, for example, represent a second analysis team, reviewing and scrutinizing the first analysis, or it could be a stakeholder with some interest in the decision to be made. Let us first consider the second analysis team case.

This second group would review all relevant aspects of the description (C',Q,K_S,K). It could, for example, act as a red team (devil's advocate) by:

- Searching for unknown knowns, i.e. events that are known by others but not by the original analysis group.
- Arguing for the occurrence of events that are considered to have negligible mass, according to the measure Q, typically negligible probability.
- Checking that relevant signals and warnings have been properly reflected.

For the leakage example, we can imagine that the second analysis group is onshore. Necessary communication with the offshore installation is carried

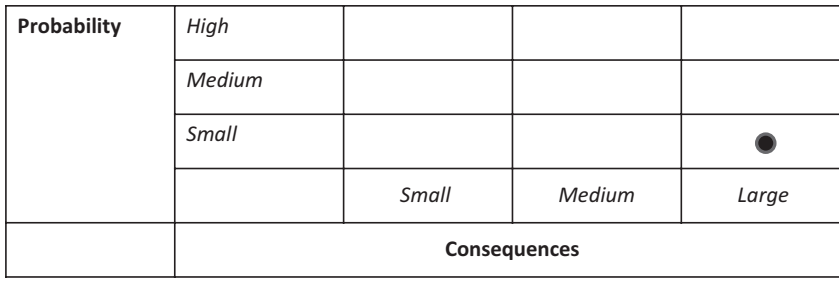


FIGURE 5.7 Consequences, probability and strength of knowledge for the hydrocarbon leakage example, when integrating judgements from a second analysis group (based on Aven 2016c)

out by video and emails. The members of this second group have experience from similar operations and technical expertise relevant to the critical operation. Based on experience and knowledge of similar leak situations, the second analysis group questions the assumption that a leakage of stabilized oil would not result in significant gas evaporation. They argue that the given assumption is wrong.

In this example, there is disagreement among the experts as to whether gas will be evaporated. It is decided to assign a weak score for the strength of the background knowledge K. The risk matrix is updated, as shown in Figure 5.7 (dark indicating weak strength of knowledge). The consequences category is changed to high.

In this case, the result was critical for the decision-making. New insights were brought to the table, and the planning of the operation had to be reconsidered.

This second-round analysis process can be quite resource-demanding, but the whole process should of course only be used in selected situations when the criticality is considered high.

Now, consider a situation where K_{S1} refers to judgements of the strength of the knowledge K conducted by a stakeholder with some interest in the decision to be made, a stakeholder who is not a risk analyst. In this situation, the above score system can also be used. Judgements of the five criteria 1–5 can be provided and added to the risk description (C',Q,K_S,K).

Note that when conducting the judgement K_{S1}, the other experts (stakeholders) may or may not base this on the analyst team judgement K_S, depending on the situation and the purpose of the judgement K_{S1}.

The decision-maker's (manager's) judgement of the strength of the knowledge K and other quality features

The decision-maker is not in general an expert on risk analysis and will simply have to acknowledge the risk characterizations of the risk analysts,

with or without the input from other experts, as discussed in the previous section – he/she is not able to scrutinize the technical approach and methods used. Nonetheless, the decision-maker needs to make his/her own judgement about a number of issues, such as:

- The strength K_D of the knowledge K.
- The implications of the analysts' and experts' results, taking into account the limitations of the analyses, for example that the analysts lack important knowledge about the system studied.
- The implications of the analysts' and experts' judgements of the strength of the knowledge K, for example the weight to be placed on the uncertainty characterizations Q when the background knowledge is considered rather weak.
- The risk related to deviations to key assumptions made.
- The quality of the analysis team, for example their experience and competence, both concerning the system studied and as risk analysts.

These are issues that the decision-maker takes into account in the so-called *decision-maker's review and judgement*, which is included in many models for risk decision-making, for example the model by Hansson and Aven (2014), presented in Figure 5.8 (see also Chapter 2). The broad risk evaluation represents professional judgements within the risk analysts and experts, reflecting insights about the system studied, as well as judgements about the risk characterizations and relevant decision criteria. An alternative perspective, but with similar features, is presented by Rosqvist and Tuominen (2004a); see Figure 5.9, which shows an adjusted version of the one developed by Rosqvist and Tuominen (2004a) (see also Rosqvist 2010). 'Concern assessment' is a term taken from the risk governance framework of IRGC (2005). It can be viewed as a systematic process to comprehend the nature of effects and changes to the socio-economic environment and to express and evaluate these effects/changes and associated uncertainties. For the present discussion, the *quality judgement* part is the most interesting one. It reflects similar aspects to those of the decision-maker's review and judgement. According to Rosqvist and Tuominen (2004a), the quality relates to confidence in the results and recommendations provided by the risk assessment. Typical questions that are raised in the quality judgements are:

- Is the scope of the assessment complete?
- Are the means of analysis and the logic of inference credible?
- Is it possible that the risk characterizations lead to unjustified decisions?

Based on the answers to such questions, the decision-maker seeks evidence as to whether or not the risk assessment is sound.

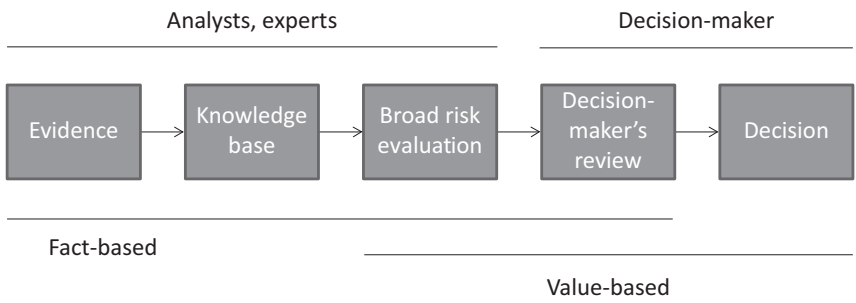


FIGURE 5.8 The role of the decision-maker's review in the decision-making process (based on Hansson and Aven 2014)

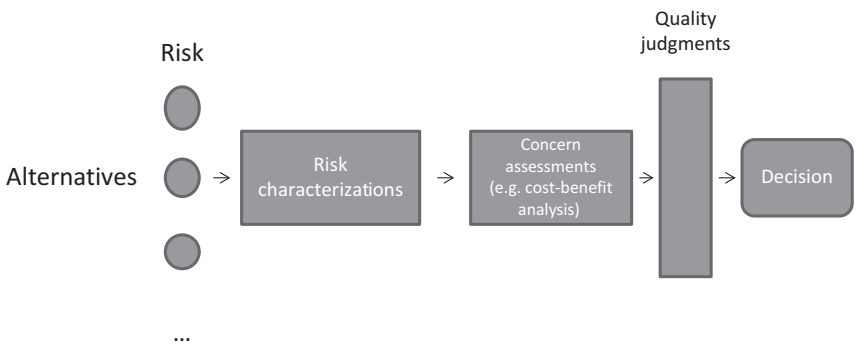


FIGURE 5.9 Risk decision model inspired by Rosqvist and Tuominen (2004) (based on Aven 2016c)

Key concepts in this respect are the reliability and validity terms, as discussed in Section 5.1.

The decision-makers and managers are not in general risk analysts and experts in this field and are not able themselves to evaluate the degree to which the risk assessments at hand meet the reliability and validity criteria. However, they should be informed about general insights that exist on this topic; for example, they should be aware of these common validity problems:

- important risk factors may be hidden in the background knowledge
- the risk and uncertainty assessments may not be complete
- hazardous situations could be overlooked.

The judgements of the strength of knowledge can be understood as an assessment of this risk, seen from the analysts' (and other persons') perspective. It provides an input to the decision-maker's and the manager's overall judgement. It is just an input, as it is limited by these groups' insights, competence

and methods. The decision-maker (manager) has to question the degree to which all relevant input has been provided: could there have been data, information and knowledge available somewhere that should have been collected? And perhaps more work should be done to gain relevant data, information and knowledge (for example, through testing and research).

Hence, the decision-maker (manager) needs to think about the overall quality of the analysis team, their experience and competence concerning the system studied and their role as risk analysts and experts. He/she needs to reflect on the status of the analysis work in general for the activity considered, for example within the organizational unit. What are the competence and training standards? What is the culture like? Is there an excellence attitude? Are improvements highlighted, etc.?

Assessing all these aspects represents a huge challenge for the decision-maker (manager). It is tempting to try to avoid such assessments and let the assessment prescribe what to do, going from a risk-informed situation to a risk-based one. In this way, if their actions turn out to be wrong (poor), they can claim absolution on the basis that "We did what the numbers told us to do. If the numbers were wrong, it's the analysts' fault" (Aven 2012d). There is, however, no way for the decision-maker and manager to escape from the responsibility – the use of a risk assessment to prescribe the decision-making cannot be justified; there will always be aspects not reflected in the assessments; it is the decision-maker's and manager's job to make the decision, and they must give the proper weight to the assessments. Then they need to understand what these assessments are producing and what their constraints are.

For the leakage example, in the case of the additional analysis not being performed, the decision-maker should carefully reflect on the uncertainties raised. These could be seen as a signal to look further into the situation, and a review by another organizational unit could be a natural action. We have, however, to acknowledge that there are so many signals and warnings that could lead to such additional reviews that it would be impossible to carry out all of them. Some sort of structure and screening is therefore needed. Some examples of such structures are presented in Aven (2013e), linked to risk acceptance criteria and the ALARP principle (ALARP: As Low As Reasonably Practicable), where the strength of knowledge dimension is taken into account. The key is to avoid direct mechanical decision processes, which do not take into account judgement of the background knowledge; see also Chapter 7.

5.5.4 Discussion and conclusions

If risk is presented by the Kaplan Garrick triplet or other probability metrics, the description represents risk as seen by the analysts (C',Q|K), conditional

on their background knowledge K. The decision-maker is concerned about risk (C,U) and needs to acknowledge that K is also subject to risk in some sense, as described in the previous sections. Hence, his/her risk description needs to be based on (C',Q,SoK,K), where SoK is some way of expressing the strength of the knowledge K supporting the (C',Q). In the previous section, we discussed what type of aspects SoK should capture and how it should be formulated. Essential input is the self-evaluation of the strength of knowledge made by the analysts, K_S, and possibly some external assessments of the strength of the knowledge K by other experts or stakeholders, K_{S1}. For the decision-maker, broader assessments are needed, however, as was discussed in the previous section. The key features to include can be summarized as:

1) The input K_S and K_{S1}
2) Own assessment of the strength of the knowledge and related issues such as risk related to deviations from the assumptions made
3) Input from relevant concern assessments
4) General quality considerations of the assessments
5) Other concerns (e.g. strategic issues, if not covered by 3)

Quantitative versus qualitative analysis

As discussed in the previous section, it is not straightforward to use all this input in the decision-making process. Both quantitative and qualitative assessments form the basis. Many analysts and decision-makers consider the former input as more objective and valuable; the qualitative is commonly referred to as subjective, lacking a scientific foundation. Such a view is, however, easily refuted. All risk descriptions are subjective or at best intersubjective among a set of analysts or experts. The point is that qualitative judgements are required to give an informative risk description, as the quantitative one fails to capture all aspects, as argued for in Sections 5.4.3 and 4.2. The choice one has to make is to stick to quantitative metrics based on (C',Q|K) and ignore important risk features or provide a broader and more complete risk description but then allow for qualitative judgements linked to K and its strength. See also discussion in Section 3.1.

The above analysis describes a practical approach, seeking to improve the decision basis. As for any risk analysis, there are limitations on how many teams and perspectives can be added to the analysis, but the risk related to, for example, unknown knowns, still has to be addressed by the decision-maker. A specific analysis group can to a limited degree address this risk.

The analysts have a responsibility to adequately inform the decision-makers about the risk and the limitations of their analyses. This includes

the need for reflections on the strength of knowledge when using the results of the risk analyses in the decision-making context. Following the ideas of the present analysis, an improved basis can be obtained for how to communicate the limitations and the issues for the decision-makers to take into account which have not been addressed by the analysts.

It is of course impossible to address all extreme/minority views and judgements. Some measure of the impactfulness of the extreme views and judgements for decision-making might be warranted before analysis proceeds, as addressed by, for example, Karvetski and Lambert (2012).

Conservatism

In some cases, when the issue concerns whether or not to accept a solution, conservative assumptions are often referred to as a useful tool to reduce the risk related to some background knowledge (Rosqvist and Tuominen 2004a). If the decision criteria are met with conservative assumptions, one should be confident that the system is in fact a safe system. There could of course be cases where such an approach could be useful, but care must be shown in not using best judgements in all parts of the assessment, as the results are then not easily interpreted. We discussed the topic in detail in Section 5.2. One may adopt some conservative assumptions, but how conservative should they be, and which quantities should be covered? There are typically a large number of possibilities, and one can easily be misled into thinking that the system is safe because some conservative assumptions have been made but fail to reflect uncertainties and lack of knowledge linked to other quantities. It is better in general, therefore, to strive for balanced risk descriptions and let the policies for treating the risk take the uncertainties into account. Cautionary policies are often implemented to deal with risk and uncertainties; being explicit about why such policies are implemented is more easily justified when the risk description seeks to provide fair characterizations of the uncertainties.

How the decision-makers will give weight to the different levels of the strength of knowledge will depend on the other risk description elements, i.e. (C',Q), and aspects like those mentioned at the beginning of this section, including points 3–5. One issue of special interest here is the question of what means and tools could be used for making judgements about when and to what extent the knowledge should be strengthened, to improve the decision basis.

The main points addressed in the present discussion in Section 5.5 are:

– The analysts' conditional risk description (C',Q|K) does not adequately inform the manager and decision-maker, as the 'risk' associated with K is not captured.

- The manager and decision-maker also need to be informed about the 'risk' related to K and make their own judgements about it.
- This can be done by deriving a risk description (C',Q,SoK,K), where SoK are ways of expressing the strength of the knowledge K supporting the (C',Q). Examples of how SoK can be developed are shown in the previous section.

It is an important research task to develop methods for describing this 'risk' linked to K. The ideas presented here represent one approach and are to be seen as initial attempts to meet this challenge.

6 Risk perception and risk communication

This chapter first discusses risk perception, then risk communication.

6.1 RISK PERCEPTION

According to SRA (2017b) (refer to items 13 and 14 in Section 3.1.1),

> Risk perception refers to a person's subjective judgement or appraisal of risk, which can involve social, cultural, and psychological factors. Risk perceptions need to be carefully considered and incorporated into risk management, as they will influence how people respond to the risks and subsequent management efforts. Risk perception studies are important for (i) identifying concerns but not necessarily for measuring their potential impacts and (ii) for providing value judgement with respect to unavoidable trade-offs in the case of conflicting values or objectives.

The risk field builds on a huge literature on risk perception and related behavioral decision-making research. This literature constitutes an important basis for the science of risk analysis. The risk perception research has identified a set of biases (heuristics) in people's ability to draw conclusions from probabilistic formulations and information (see e.g. Tversky and Kahneman 1974, Rohrmann and Renn 2000, Renn 2008). The risk perception research has also revealed different meanings of risk, depending on the context in which the term is used (see e.g. Slovic 1987, Renn 2008). People's understanding of risk extends beyond the professional characterizations based on consequences (loss) and probabilities. These characterizations provide a too narrow perspective on risk, as important risk-related aspects for

the decision-making, such as affect, controllability and familiarity, are not considered. Closely related to this conclusion is the well-known dichotomy between the two modes of thought: *System 1*, which operates automatically and quickly, instinctively and emotionally, and *System 2*, which is slower, more logical and deliberative (see e.g. Zajonc 1980, Epstein 1994, Sloman 1996, Pidgeon 1998, Chaiken and Trope 1999, Kahneman and Frederick 2002, Slovic et al. 2004, 2007, Wilson and Arvai 2006, Keller et al. 2006, Kahneman 2011). The message is that both System 1 and System 2 types of thinking are needed to properly react to and manage risk.

The literature on risk perception has demonstrated that mean values of the perceived seriousness of risks often deviate from mean or medium expert judgements or assessments of the same risks (Slovic 1987, Boholm 1998, Sjöberg 2000, Renn 2008). Politicians, hence, face a dilemma: if they base their risk policies on the expert judgements alone, they may lose public support; if they take the perceptions as guidance for their decisions, they are likely to spend their resources dedicated to risk reduction unwisely. They may finance costly risk reduction measures that are high on the public agenda but may only marginally improve human health and the environment, and they may not address serious risks because these are not perceived as serious in the public eye. It is evident that, from a normative perspective, knowledge about individual perceptions of risk cannot be translated directly into risk-reduction policies. Given the many insights from psychological research into the fact that perceptions are based partially on biases or ignorance, it does not seem wise to use them as yardsticks for risk reduction (Fischhoff et al. 1981, Slovic 1992, Wilson and Arvai 2006, Aven and Renn 2010). In addition, risk perceptions vary among individuals and groups: whose perceptions should be used to make decisions on risk?

At the same time, however, these perceptions reflect the real concerns of people and include the undesirable effects that 'technical' analyses of risk often miss. It is true that laypeople's views of risk are intuitive and less formal and precise than experts' statements. However, as Paul Slovic observed, "Their basic conceptualization of risk is much richer than that of experts and reflects legitimate concerns that are typically omitted from expert risk assessments" (Slovic 1987, p. 282).

In fact, laypeople's risk judgements indicate more than just the perception of riskiness. They reveal global views on what matters to people, on technological progress, on the meaning of nature and on the fair distribution of chances, benefits and risks. Facing this dilemma, how can risk perception studies contribute to improving risk policies? Pertinent benefits of revealed perceptions may be as follows (de Marchi 2015, Fischhoff 1985):

- They can identify and explain public concerns associated with the risk source.
- They can elucidate the context of the risk-taking situation.
- They can enhance understanding of controversies about risk evaluation.
- They can identify cultural meanings and associations linked with special risk arenas.
- Based on this knowledge, they can be useful when articulating objectives of risk policies that go beyond risk minimization, such as fairness, procedural equity and institutional trust.
- They can indicate how to design procedures or policies that incorporate these cultural values into the decision-making process.
- They can be useful in the design of programmes for participation and joint decision-making.
- They can provide criteria for evaluating risk management performance and organizational structures for monitoring and controlling risks.

Risk perception studies demonstrate what matters to people. In a democratic society, the concerns of people should be a guiding principle for collective action. Context and supporting circumstances of risk events or activities constitute significant concerns. These perception patterns are not just subjective preferences cobbled together: they stem from cultural evolution, are tried and trusted concepts in everyday life and, in many cases, control our actions. Their universal nature across all cultures allows a collective focus on risk and provides a basis for communication (Renn 2008, pp. 146–7). From a rational standpoint, it would appear useful to systematically identify the various dimensions of intuitive risk perception (concerns assessment) and to measure the extent to which these dimensions are met or violated by the best available scientific methods. Many psychometric variables that matter to people are open to scientific study and scrutiny. In principle, the extent to which different technical options distribute risk across various social groups, the degree to which institutional control options exist and the level of risk that can be accepted by way of voluntary agreement can all be measured using appropriate research tools. Risk perception studies help to diagnose these concerns. Scientific investigations can determine whether these dimensions are met or violated and to what degree. This integration of risk expertise and public concerns is based on the view that the dimensions (concerns) of intuitive risk perception are legitimate elements of rational policy, but assessment of the various risk sources must follow robust scientific procedures on every dimension.

Moreover, designing policies about advancing, supporting, and regulating risks requires trade-offs between different concerns. Such trade-offs depend upon both context and the choice of dimension. Perception research

offers important pointers concerning the selection of dimensions for focus (Rayner and Cantor 1987). For example, the aspect of fairness, which is rated highly among people as an evaluation tool for the acceptability of risks, plays a significant role in such trade-offs and in weighting the various dimensions. In their roles as risk assessors, experts have no authority to select these dimensions or to specify their relative importance. This is where formal methods reach their limits. The multidimensionality of the intuitive risk model prevents risk policy from focusing one-sidedly on the minimization of expected impacts or related metrics.

In essence, policy-makers should be aware of public perception and concerns and take them as a legitimate input to risk management and regulation. Yet, concerns may be associated with problematic or even wrong (poor) causal models or they may simplify these models to such a degree that they are not useful for effective risk management and regulation. Thus, as stated in SRA (2017b), public input is important for (i) identifying concerns but not necessarily for measuring their potential impacts and (ii) for providing value judgement with respect to unavoidable trade-offs in the case of conflicting values or objectives.

6.1.1 The difference between risk, professional risk descriptions and risk perception

Risk perception as used in this book is not the same as risk and professional descriptions or characterizations of risk. This is in contrast to, for example, scientists advocating cultural theory and constructivism, who state that *risk is the same as risk perception* (Jasanoff 1999, critical comments in Rosa 1998). Risk coincides with the perceptions of it (Douglas and Wildavsky 1982, Freudenburg 1989, Rayner 1992, Wynne 1992). Beck (1992, p. 55) states that "because risks are risks in knowledge, perceptions of risks and risk are not different things, but one and the same".

However, acknowledging that any risk characterization is knowledge-based and subjective/intersubjective does not mean that risk is the same as perceived risk. For example, a risk assessment can describe risk using knowledge-based probabilities, but these probabilities do not reflect perceptional aspects like fear and dread. The analyst may conclude that the probability of an event occurring is 0.1, meaning that he or she has the same degree of belief that this event will occur as randomly drawing a specific ball out of an urn comprising ten balls. The assignment is based on some knowledge (data, information, justified beliefs) but does not include aspects linked to how the assigner likes/dislikes the event or, for example, fears its consequences. A professional risk analyst is able to make a probability assignment without being influenced by such perceptional aspects. In practice, there

could of course be assignment problems, for example as a result of overconfidence and group-thinking (e.g. Pidgeon 1998).

Risk perception also sometimes covers judgements of the acceptability of risk, which makes the difference between risk perception and professional risk descriptions even more evident. The concept of risk and a professional description of it do not include judgements about risk tolerability or acceptability.

To discuss the issue in more detail, we return to the book, *Thinking, Fast and Slow*, written by Kahneman (2011), in which the author presents an example related to suicide bombings on buses in Israel in the period from 2001 to 2004; see Section 1.4. In this example, a professional analyst describes or characterizes the magnitude of the risk through the death rate and associated probabilities. From this basis, it is demonstrated that the risk is not higher than for activities that we normally conduct, like driving, and hence the risk associated with taking buses should also be acceptable or tolerable. System 2 thinking is used for this analysis. A bus rider, we call him John, is still concerned. His quick and intuitive judgement about risk is that it is too high; he will not take the bus if he can avoid it. He senses the uncertainties in relation to taking the bus – next time it could be his bus.

There are many factors or issues that could affect this System 1 thinking. For example, his risk judgements could be amplified (Kasperson 1992, Kasperson et al. 1988), as a result of the media, biases or heuristics (Tversky and Kahneman 1974) – for instance, the availability heuristic would make the most recent events the most salient ones – and his level of trust in the information and its sources.

His risk perception is based on System 1 thinking – which is intuitive, associative and automatic – which concludes that the risk is too high, and the bus-taking should be avoided.

Does this thinking express risk in some sense? Yes, it is an example of a risk perception reflecting the assessor's subjective judgement of the risk, which allows for considerations of affects and also includes issues of acceptability/tolerability (Renn 2008). But not risk *per se*? It depends on what risk *per se* is. If risk *per se* is the death rate or associated probabilities, the System 1 thinking is clearly not very informative. However, if risk *per se* is the potential for an unwanted event, or the possibility of such an event, or "damage + uncertainties" as in Chapter 4, the conclusion is not so straightforward. The potential, the possibility or uncertainties: we certainly have these in this case. John faces uncertainties – it is not known whether his bus will be attacked or not; there is the potential, the possibility. His System 1 thinking is perhaps responding to these uncertainties, this potential and possibility. So, perhaps the thinking nonetheless brings some useful information to the decision situation.

And if risk *per se* captures uncertainties, the potential and possibility, it probably also affects the way we should judge the magnitude of the risk. There is a gap between uncertainties, the potential and possibility, on the one hand, and a historical rate or related probabilities, on the other. The literature is filled with analyses and reflections on the issue of transforming uncertainties, potentials and possibilities into some measurement tool (e.g. Lindley 2006, Dubois 2010, Flage et al. 2014); see Section 4.2. Probability is the most common tool, but it has limitations, and many alternatives have been suggested. There are different views on what are the most suitable approaches and tools in this respect, but there should not be much discussion on the need to show some humility in being able to measure the risk. It has to be acknowledged that any measurement of uncertainties, potentials and possibilities would mean some level of subjectivity and would raise several issues. For example, if the historical death rate is used in our example to measure risk, it is based on an assumption of stability in the level of attacks. But who knows whether this assumption will hold for the period that John considers? It could increase or decrease, and the form of attacks could change. The next day, one or more new campaigns of attacks could be launched. These are issues that John faces and that could be reflected in his System 1 thinking, as well as in his System 2 thinking. John may be informed about the historical rate, but the poor knowledge that characterizes the situation can get System 1 to react, avoiding the risk.

With large uncertainties and poor knowledge about what is happening, is not cautionary thinking quite natural? Yes, it is. We do not walk on the ice on a lake if we do not have reliable information about its safety (how thick the ice is). Is not the situation similar in the bus example? The knowledge is also rather poor. System 1 reacts – the risk could be judged as too high. Kahneman drove away faster from the bus than he usually did when the light changed, as his System 1 reacted instinctively and automatically to the uncertainties and risk. Why should he be chagrined by this fact?

The traditional risk assessment and management thinking highlights the calculated death rate and gives little weight to the uncertainties. According to such a perspective, one could be chagrined, as risk then is considered minor. Adopting a different risk perspective: risk could, however, be judged as high, just by allowing for a broader understanding of risk.

It may be argued that the above analysis is very incomplete in that it is not only uncertainty that is relevant for the decision-making. We know from the risk perception and behavioural decision-making research that aspects like affect, control, familiarity, catastrophic potential, etc. are important. However, the focus here is not descriptive decision-making but normative decision-making: how we should make decisions. The idea is to separate what are pure risk judgements and characterizations, and what are risk

perceptional aspects, for example fear. Decision-makers may have different attitudes concerning the weight to be given to such aspects. To change professional risk assessment and management practice, we should be clear what we are trying to add: judgements of uncertainty or perceptional aspects.

In this book, a clear distinction is made between the risk characterization (C',Q,K) and risk perception. The risk characterization provides 'pure' judgements of the consequences and uncertainties, without adding feelings and value judgements related to how one likes or dislikes C and U. Risk perception, on the other hand, is a personal judgement of risk, also including such aspects. In the above example: taking the bus, John will face risk, as there are some values at stake – some consequences of the activity – and uncertainties. He may be filled with fear and his risk perception be very much flavoured by this. A risk characterization would, however, be restricted to pure judgements of the consequences and uncertainties and not be affected by perceptional aspects like fear.

6.1.2 Methodological issues related to risk perception research

Risk perception research studies how people perceive risk. This is conducted by conceptual and empirical analysis. An approach – a theory or model – is developed, which is to describe the 'world', i.e. how people in real life perceive and make decisions in relation to risk. Then, data are generated using different methods, including making a survey, in which information from a sample of individuals is gathered, for example by questioning how they perceive risk associated with specific activities (Sjöberg 2003). The data are interpreted in view of the approach (theory, model) used. See discussion in Section 3.2.2 of different types of research methods. Statistical inference represents a basic methodological framework for much of this research.

As an example, let us consider the so-called psychometric paradigm (Fischhoff et al. 1978, Slovic 1987). The approach aims at identifying the key factors that influence the perception of hazards. Starting from a set of factors – voluntariness of risk, immediacy of effect, knowledge of risk of those who are exposed, scientific knowledge, control over risk, newness, number of people killed in an incident, dread potential and high severity of an incident – the statistical analysis reveals two main contributors: dread and newness. From this result, a map is presented, which depicts a number of hazards in a two-dimensional space with these two factors. It is a map that is easy to understand and is one of the most popular figures in the science of risk analysis.

However, as for all statistical analysis of this type, there are pitfalls. The approach seems to indicate that the map fully explains laypeople's risk

perceptions, but this is not the case; see discussions in, for example, Sjöberg (2003) and Siegrist et al. (2005). The approach produces a model of the world and, as for all models, it has limitations and weaknesses. Yet, it can be useful for our understanding of how people perceive risk. There is and needs to be a continuous discussion about the research and what is the current knowledge on risk perception.

As highlighted above, the risk perception research has demonstrated that people's understanding of risk extends beyond the professional characterizations based on consequences (loss) and probabilities and, in particular, expected values with these two dimensions multiplied. As discussed in Section 6.1.1, traditional professional risk characterizations need to be extended, to make informed decisions in the face of risk, mainly for two reasons:

1) These characterizations do not capture all aspects of uncertainties (refer to discussion in Section 4.2).
2) Judgements about what risk to accept need to be seen in relation to other concerns, not only risk.

Risk perception takes into account the full spectrum of uncertainties, and includes judgements of acceptability. Hence, we cannot expect risk perception results to be comparable to professional judgements of risk, which make a clear distinction between risk characterizations and how to handle the risk.

6.2 RISK COMMUNICATION

We refer to the basic principles of risk communication in Section 3.1.1 (items 15–19). There is a huge body of literature on risk communication addressing this type of issue and related ones; see, for example, Covello et al. (1986), Fischhoff (1995), Bier (2001a, b), Bostrom and Löfstedt (2003), McComas (2006), Renn (1998a, b), Visschers et al. (2009) and Pidgeon and Fischhoff (2011). This literature provides concepts, theories, frameworks, approaches, methods and models for communicating risk, as we discussed in Section 3.1 (generic risk communication and risk analysis B). It also covers studies of risk communication for concrete activities (applied risk communication and risk analysis A), using the B type of knowledge. The research conducted is conceptual with strong elements of empirical work, see Section 3.2. Beyond the principles highlighted by SRA (2017b), a number of recommendations have been formulated on the basis of the risk communication research. As an example, Bier (2001a), presents the following recommendations in relation to designing risk communication messages:

> View risk communication as an opportunity to demonstrate trustworthiness and an open, responsible, and caring attitude. Listen to audience concerns before attempting to impart new information. Use risk comparisons with caution:
>
> 1. Consider presenting comparisons of the same risk at different times (e.g. a few years ago vs. now), comparisons with other causes of the same disease or injury, and comparisons with unrelated risks, such as the risk of lightning.
> 2. Avoid comparisons with risks that are generally viewed as trivial, such as the risk of eating a few tablespoons of peanut butter.
> 3. Pilot test risk communication messages (especially risk comparisons) on a limited basis before using them more widely, to ensure that they are easily understood and not misinterpreted. This is particularly important in situations of distrust.
>
> (Bier 2001a)

Reference is made to the above publications for other examples.

In the following, we will look more closely into some of the basic risk communication principles as formulated by items 15–19 in Section 3.1.1. The risk communication literature builds strongly on the concepts of risk and probability, and we will therefore focus on these concepts and discuss how risk communication is closely related to the science of risk analysis. We will also provide some comments concerning the policy of openness and transparency in risk communication.

6.2.1 Perspectives on the nexus between good risk communication and high scientific risk analysis quality

In general, successful risk communication can be said to require "an understanding of the target audience, including the best means for reaching the audience: a credible or trusted source; and a message that has ideally been pre-tested to ensure its effectiveness" (SRA 2017b). Seldom is the scientific quality of the risk analysis questioned. The sources can be credible or trusted, but the scientific risk analysis quality can be poor. For example, the risk communication can be based on a scientifically unsound risk characterization yet be communicated successfully from a pure communication point of view. Good risk communication cannot, however, be seen in isolation from the broader process of risk analysis and management. The present discussion provides some reflections on this topic, the main aim being to strengthen the argumentation for the thesis that scientific and foundational issues of risk analysis are critical for the successful communication of risk. Several examples are used to demonstrate this thesis.

To be somewhat more concrete, think about a hypothetical case, where a risk assessment for a process plant is conducted by a recognized consulting company and the results are communicated to the public and the decision-maker. A key result is that the risk – expressed as a computed probability – is found acceptable, according to some defined criteria. The activity studied is judged to be safe. Dialogue and interaction among all relevant stakeholders are also conducted. All parties, including the decision-maker, consider the consultancy company to be a highly credible and trusted source and conclude from this that they have been adequately risk informed and the risk communication process has been solid and positive in all respects. All involved perceive the communication as successful.

As another example, consider the current risk and threat level characterizations in relation to security issues; see for example UK (2018) and PST (2018) (further details are given below). People are informed by the authorities that the threat level is low, the reference being a low-judged likelihood. It is probable that the police security services have a good basis for their judgements, and it can thus be argued that the risk communication is successful – people are adequately informed.

But are these perceptions and judgements really enough to conclude that the risk communication is successful? No; successful risk communication cannot be seen as separate from the scientific quality of the risk assessments and the risk characterizations. It is necessary to question the extent to which the risk assessment and the risk characterization are in line with the scientific knowledge generated by the risk analysis field. There will always be discussions about what is the current risk analysis scientific knowledge, yet it is important to acknowledge that some quality references exist that extend beyond individual perceptions. The analysis group members may be confident that they are applying appropriate risk analysis concepts, approaches, principles and methods, but this does not mean that this is in fact the case, as the reference is the risk analysis science.

For example, in the security example, it can be argued that risk communication based on likelihood judgement alone can mislead the public. The problem is that the strength of the knowledge supporting the judgement is not really covered by the likelihood judgements used to characterize and communicate the risk level, as will be thoroughly discussed below.

As another example, consider climate-change-related risk and the associated risk communication of the Intergovernmental Panel on Climate Change (IPCC). For many people, the IPCC is indeed a credible and trusted source. Based on thorough analysis, involving a number of scientists, the IPCC has produced extensive characterizations of climate-change-related risk and uncertainties. However, from a risk science perspective, it can be argued that this risk communication is poor in many ways (refer to Aven and

Renn 2015). For example, the IPCC uses the likelihood/probability concept to express important findings, for instance that it is extremely likely (at least 95 per cent probability) that most of the global warming trend is a result of human activities (IPCC 2014a). The IPCC does not, however, provide a clear understandable interpretation of the likelihood/probability concept. The consequences are that people read this type of statement in different ways and have difficulties in understanding what the probability really expresses: does it reflect fundamental variation in physical phenomena, differences in expert judgements, different views about specific issues or something else?

If we read the media interpreting the IPCC work, the impression is that the IPCC expresses that science states that global warming takes place and is a result of human activities; the uncertainties are very small and can be basically ignored: the experts are confident that the statements referred to are true. However, the IPCC reports stress that likelihood and confidence statements should not be mixed ("Confidence should not be interpreted probabilistically" (IPCC 2010)). The 95 per cent probability statement is of course also related to confidence, but the IPCC reports seem to indicate that this is not the case. Thus, a deeper look at the IPCC platform on risk and uncertainty reveals that the analysis has some serious weaknesses. Acknowledging these, can we still argue that the risk communication is successful?

Clearly, what 'successful' means depends on what the reference is. The issue has been thoroughly discussed in the risk communication literature (e.g. Covello et al. 1986, Zimmennann 1987, Keeney and von Winterfeldt 1986, Renn and Levine 1991, Kasperson 1992, Fischhoff 1995, McComas 2006, Renn 2008). Examples of risk communication objectives include: enlightenment function, right-to-know function, attitude change function, legitimation function, risk reduction function, behavioural change function, emergency preparedness function, public involvement function and participation function (Renn and Levine 1991). Increasing trust and credibility is often seen as a key objective of the risk communication, and trust and credibility are also prerequisites for many other objectives (Renn and Levine 1991). Trust and credibility depend on how the receiver perceives the source when it comes to factors like competence, objectivity, fairness, consistency and faith. It is expected that the communicator conveys accurate, objective, and complete information (Renn and Levine 1991).

There is, however, a potential gap between what is perceived as competence, objectivity, etc. and what the scientific field claims. In the above examples, the sources may be viewed as trusted and credible, yet the risk communication can be considered unsuccessful from a risk science perspective.

In the following, this issue will be discussed in further detail: the nexus between risk communication and the scientific quality of the risk analysis, using the above examples as points of departure. The main aims are to

achieve increased awareness of this issue, as it is considered under-focused on today, as well as to obtain new insights into risk communication's dependencies on the scientific and foundational issues of risk analysis. The discussion is based on the conviction that current risk analysis practice is subject to many weaknesses of a conceptual and fundamental character, which have severe implications for the quality of the risk communication and risk management, as indicated by the above examples. Probability is a key concept in risk and uncertainty analysis, but lack of precision in the understanding and use of this concept hampers risk communication and management in many situations. The reference for what is good – high-quality – risk analysis is represented by the most warranted statements or justified beliefs that the risk analysis knowledge field can produce; refer to discussion in Chapters 2 and 3.

The IPCC risk communication

The IPCC aims at informing governments and decision-makers at all levels on scientific knowledge about climate-change issues. Their work is, to a large extent, about risk. The communication can be viewed as successful, in the sense that most governments are now taking serious action in line with the main conclusions made by the IPCC. However, the scientific quality of the risk assessments and characterizations – and, hence, also the related risk communication – can be questioned.

Risk and probability are fundamental concepts in the IPCC work. However, clear definitions are not provided. As referred to above, it is a key message of the IPCC that it is very likely that most of the global warming trend is a result of human activities. A probability of 95 per cent is used to express this, but no interpretation is presented. The concept of risk in the IPCC works refers to probability but with no interpretation of probability; also, the concept of risk become undefined and vague. Equally important, significant aspects of risk are not really communicated. The point being made is that, to be used in relation to climate-change issues, a probability has to be viewed as a subjective probability, which is conditional on some knowledge. This knowledge can be more or less strong and even erroneous. This fact creates two additional dimensions of risk: first, a need to characterize the strength of this knowledge and, secondly, a need to consider surprises relative to the knowledge available (SRA 2015b, 2017b, Aven and Renn 2015). The IPCC works are not explicit on these dimensions, although the former is discussed in relation to statements when referring to evidence and agreement among experts. The problem is, however, as was mentioned above: there is no link between the probability judgements and the strength of knowledge judgements in the IPCC framework. The risk analysis science

clearly shows that such a link exists and is essential for understanding risk (SRA 2015b, 2017b, Aven and Renn 2015), refer to Chapter 4.

Most governments and decision-makers seem to trust the IPCC and its scientific results and find the IPCC to be a credible source for communicating the climate-change-related risks. The concerns raised by risk analysis have not influenced this trust and credibility. It can be argued that these concerns are not of a significance that changes the overall important conclusions from the IPCC: rather, they should be seen as details on a technical level.

However, this type of reasoning is easily rebutted. It represents a dangerous attitude to science, which, per definition, seeks to identify and use the most warranted statements and beliefs that the knowledge disciplines can produce (Hansson 2013a, Hansson and Aven 2014). Risk analysis is a key science in relation to all types of risk knowledge generation, including climate-change-related risk. One of its main focus areas is risk conceptualization and characterizations. It provides authoritative guidance – the key principles – on how risk should be best described to inform decision-makers and other stakeholders. Violations of these principles can strongly influence the way risk is understood.

For example, when using the term 'probability of 95 per cent' to express that it is very likely that most of the global warming trend is a result of human activities, it matters greatly whether this is a statement reflecting some objective physical phenomena in the world or whether it is the view of some experts. The IPCC is not clear on this point but indicates in a rather imprecise way that the probability is linked to variation and, thus, some physical phenomena. This type of interpretation gives the probability statement a stronger scientific basis than if we are to interpret the probability as a subjective probability. Although the latter type of probabilities can be given a rigorous foundation (Lindley 2006, Section 4.2), it represents a challenge in risk communication, as it is a judgement made by someone.

Openness and traceability on such matters characterize high-quality risk analysis. However, these issues are not discussed in the existing IPCC documents. There is no reason to believe that the current imprecision on key concepts in these documents is a deliberate policy to strengthen the objective authority of the IPCC findings. However, the imprecision opens the door to legitimate criticism, as the 'objective variation type of interpretation' is not justified. In fact, on the basis of the scientific risk analysis work referred to, the risk analysis science would conclude that it cannot be justified, as there is no objective foundation for such a probability in a case like this. Knowledge-based probability is the only one that can be meaningfully defined. According to this thinking, the assessor has a strong belief that most of the global warming trend is a result of human activities, but it must be acknowledged that this is a belief conditional on some other

beliefs (knowledge). It does not mean that the statement is true in at least 95 out of 100 cases, as is often used to explain probabilities. This type of interpretation has no meaning in this context. Rather, we must think of the uncertainty and degree of belief as comparable with drawing a red ball randomly out of an urn comprising 100 balls, of which 95 or more are red. The interpretation does not reflect any type of variation or features of the real world, although variation and such features can be used as input to the judgements of the uncertainties.

On this basis, it can be claimed that the current IPCC risk communication misinforms decision-makers and other stakeholders. The risk communication fails from a risk science perspective.

Solidity is a basic requirement for a high-quality assessment, as was discussed in Section 3.1.1. Not being precise on the meaning of key concepts violates this requirement. This is not about semantics as such but about the fundamental risk thinking that has considerable influence on how the results and findings of the IPCC work are reported and communicated. It is also about lack of validity, as the aim of the IPCC work is to adequately characterize risk. Important aspects of risk are neither explained nor addressed, as discussed above and in greater detail in Aven and Renn (2015).

Security risks

Consider as an example the UK Secret Services' approach to expressing threat levels (UK 2018). Five categories are used: "LOW means an attack is unlikely, MODERATE means an attack is possible but not likely, SUBSTANTIAL means an attack is a strong possibility, SEVERE means an attack is highly likely, and CRITICAL means an attack is expected imminently" (UK 2018). In Norway, a similar categorization is used by the Norwegian Police Security Service (PST): "*Very likely*: There is very good reason to believe, *Likely*: There is reason to believe, *Possible*: About as likely as not, *Unlikely*: There is little reason to believe, *Very unlikely*: There is very little reason to believe" (PST 2018).

Now, suppose a case where the assessor's belief that an attack will occur is considerable but far from 50 per cent, and the supporting knowledge is very strong. How should the assessor classify and communicate this? Using the above systems is difficult. Of course, any classification system would have weaknesses and limitations, but the current systems mix likelihood judgements and the knowledge supporting these judgements. The result is confusing terminology and communication. An attack is always possible, and what does "strong possibility" mean? Using subjective (knowledge-based) probabilities – preferably as intervals – clarity can be obtained, as well as more informative communication. The assessors' judgements are

based on the available intelligence and possible attackers' capabilities and intentions, but, using the current classification systems, the strength of this information and knowledge is not communicated to the public in an informative way – important aspects of risk are suppressed. We again see how risk analysis insights are important, to ensure good risk communication. See Aven (2013c) for an alternative threat level classification system based on the ideas presented in this book.

Industry safety case

We return to the industry example introduced above. In this case, all involved parties found the risk communication successful in all respects, but, nonetheless, there could be reasons to question the quality. The approach taken serves the interests of the operator of the plant and the consultancy company, and the public and decision-makers did not have the competence needed to challenge the risk assessments conducted. The overall perception is that the risk assessment and related management processes are conducted in line with well-established standards, like the ISO 31000 on risk management. There are no incentives for the operator and consultancy company to see beyond these standards and their own in-house procedures.

There may, however, be a gap between this practice and the scientific knowledge on risk assessments. This gap can be unknown to the consultancy company or not acknowledged as a gap. Their authority as a recognized consultancy company would suffer if it became known that the approach adopted is not in accordance with the best available scientific insights. The result is that weaknesses and delimitations of the assessment approaches and methods are often suppressed.

To meet this challenge, the relevant safety agency has a responsibility. It needs to be updated on current scientific developments. However, in practice, there is often a considerable delay between the knowledge of the scientists and the regulations and industry practice. Also, the agencies may face a dilemma in acknowledging that important scientific findings on how to conduct the risk assessments exist but not implementing them in official regulatory documents. The implications are often that the agencies are also passive in relation to questioning the practice of the consultancy companies.

A debate on the risk analysis approach can still arise, as members of the public may be unhappy with the conclusion of the risk management and start to look for ways of questioning its rationale. Then, experts on risk analysis are contacted, often resulting in findings of problematic issues linked to the approach and methods used. The gap between science and practice is pointed to. There could be various motives for these experts being involved and allowing their voice to be used to challenge the consultancy companies, but usually their judgements add alternative and new perspectives to the

understanding of risk as presented by the consultancy and operator. Here is an example, inspired by discussions in Aven (2011b).

The consultancy and operator communicate that the plant is safe by referring to a derived risk level expressed in the form of probabilities of undesirable events. The argumentation is that the plant has no unacceptable risks. However, as discussed in Section 4.2, risk is in general poorly described by reference to probabilities alone. The probabilities can be based on a more or less strong knowledge, and this strength also needs to be considered and communicated, along with the probabilities. In addition, the fact that surprises can occur relative to current knowledge also needs to be addressed, as the public will be exposed to these. Not addressing these issues, as often seen, means camouflaging important aspects of risk. The public is not properly informed about the risks. The risk communication fails in informing the public.

In most cases, the public will not have the competence to challenge the consultancy companies and operators, as the risk assessments are technical and use terminology which is difficult for laypersons to understand. Yet, the risk communication cannot be judged as successful just by observing that all relevant parties are pleased with the approach taken or do not have reasons to question it. The risk science is also a relevant party and needs to be included when making judgements about the quality of the risk communication.

Discussion

Moser (2010) provides an informative review of fundamental research findings on risk communication as applied to climate change. The author distinguishes between three main categories of communication purposes. The first one concerns informing and educating people about the issue, here climate change. The second purpose is to obtain some type and level of social engagement and action, whereas the third category aims at bringing about changes in social norms and cultural values that act more broadly. Only the first one is addressed in the current discussion. The other two categories are interesting from a risk communication point of view, given the stated purpose, but defining these purposes is founded on value judgements that extend beyond the science of risk analysis.

Research on risk perception and communication has clearly demonstrated that understanding risk requires more than informing and educating people about risk estimates (Pidgeon and Fischhoff 2011). Such estimates are not enough to bring laypeople an understanding of risk in line with scientists' expectations. To affect people's behaviour is even more difficult. We know that people's risk perceptions and related decisions are affected by a number of factors and also feelings (Slovic et al. 2004, Fischhoff 1995, Pidgeon and Fischhoff 2011), but this discussion is outside the scope of the

present analysis. Here, the focus is on the scientific understanding of the concept of risk, not on how people choose to react to this risk. An interesting question is whether an enhanced risk science and related risk communication would have the potential to provide people with an improved scientific risk understanding and establish a stronger separation between people's scientific risk understanding and what are perceptional aspects. Surely, simply characterizing risk through some probability numbers would create a gap between people's risk characterization and their intuitive risk understanding, the result easily being that this 'risk gap' is mixed with the risk perceptional factors when trying to explain people's attitude to risk, as discussed in Section 6.1.1.

The critical issue seems to be that important aspects of uncertainty are not captured by current risk conceptualizations and characterizations. The industry example illustrates this clearly. The professional risk descriptions and related communications highlight probabilities and statistical expected values, and risk considerations beyond these are judged by the risk analysis professionals and the industry – often also the safety authorities – to be highly subjective risk perceptions of a different value and importance, compared to the 'objective' risk characterization produced by the scientists and analysts. However, the current risk analysis literature provides strong support for the acknowledgement that uncertainty is a main component of risk, and people's judgements of risk can, thus, be far more informative than a narrow probabilistic representation and communication of risk.

An illuminating security application is presented in Sections 1.4 and 6.1. Here, historical data are used as a reference for the risk considerations, and it is argued that, if risk is assessed as being higher than is indicated by the data, it is irrational and perceptional aspects like fear are dominating the judgements. However, people's judgements in the situations considered can equally be seen as serious deliberations of the uncertainties and risk, where perceptional aspects like fear are not an issue at all. Depending on the perspective taken, the risk communication will be completely different. The present book argues that only the latter perspective represents high-quality risk analysis.

The same type of discussion is also relevant for the climate-change case. Here, the uncertainties are clearly acknowledged and communicated by the IPCC, but based on characterizations which are not complete and convincing. First, probabilities are referred to, which are not well-defined, giving the impression that these probabilities are more scientific than can be justified. Secondly, the strength of the knowledge supporting these probabilities is not described, as the IPCC framework fails to link probability judgements and knowledge, as discussed in Section 4.2.2.

Conclusions

Successful risk communication can be defined in relation to different purposes. The present discussion focuses on the information and education purposes. Although the competence of the risk-communication sources is always an issue when discussing the success of the communication, the dependence on the quality of the risk analysis as such is seldom addressed. The above analysis has pointed to this fact and provides discussions and examples illustrating the problem.

Applied risk analysis is to be guided by the science of risk analysis, on which concepts, principles and approaches to use, to adequately analyse and communicate risk in practical cases. There will be and should be a continuous debate about what constitute these concepts, principles and approaches, but, at a specific point in time, the discipline of risk analysis needs to define and communicate what is its current knowledge. The work by SRA on these issues and the present book represent contributions to this end.

6.2.2 Risk communication in the light of different risk perspectives

A risk perspective contains the fundamental building blocks forming the understanding of risk and can be based on scientific pillars and/or more informal conceptions and judgements of risk (risk perceptions). In the following, we discuss how the risk perspectives of various actors influence risk communication in relation to processes concerned with the assessment and management of risk. Based on a set of five defined risk perspectives, we investigate how the risk perspective influences the risk communication and how and to what extent differences in risk perspectives can cause barriers and problems in the communication.

The handling of risk in society is ultimately carried out by people. A central activity for any successful risk-handling process is the exchange of risk-related information between them. Many different factors can affect how the actual risk communication takes place. The focus in the following discussion is on how the risk perspectives of the involved people can influence the risk communication. We will study five types of risk perspectives:

- The actor believes in an underlying objective risk, and risk analysts and experts provide good estimates of this risk.
- The actor believes that uncertainty is a main component of risk and that probability is a useful tool for describing the uncertainties but also acknowledges that this tool has strong limitations.
- The actor believes in an underlying objective risk based on frequentist probabilities reflecting stochastic (aleatory) uncertainties but considers

"non-probabilistic" methods to be the appropriate tool to describe epistemic uncertainties (the use of subjective probabilities is rejected unless the information is very strong). These alternative approaches include imprecise probability and so-called evidence theory (see e.g. Aven et al. 2014).

- The actor has a 'chaotic' understanding of risk, with no proper scientific basis, lacking a proper understanding of fundamental concepts like risk, probabilities and uncertainties, and/or mixing various ideas about these concepts.
- The actor sees risk as the same as risk perception.

We refer for short to these perspectives as the 'objective risk view', the 'uncertainty view', the 'non-probabilistic view', the 'chaotic view' and the 'risk=perception view', respectively. For the first three perspectives, which all have a professional/scientific basis, although founded on different pillars, there is a fundamental distinction between risk and risk descriptions carried out by experts, on the one hand, and risk perception, on the other, as discussed in Section 6.1. The perception notion includes personal feelings and affections (e.g. dread) about the possible events, the consequences of these events and about the uncertainties and probabilities, but such feelings and affections are not considered as part of the risk concept *per se* and the way risk is described when used in professional/scientific contexts.

The set of perspectives here defined is considered to reflect common perspectives seen in practice. Many perspectives other than these five exist, but, for the purpose of the present work, this set is considered to be sufficiently representative.

Of course, the objective view actor could also be aware of uncertainties and acknowledge that the different tools used have limitations. It must be emphasized that it would be possible to define several perspectives between the objective view and the uncertainty view, and also between some of the other perspectives, but, to simplify the analysis and make the points clear, attention is restricted to the five commonly adopted views presented above.

Since the risk perspective of an actor forms his/her fundamental understanding of risk, it can affect his/her risk communication. This is the issue discussed in the following analysis. We consider four categories of risk actors – a decision-maker, a risk analyst, an expert and a layman (from the general public). Using a set of communication scenarios that resemble situations commonly found in reality, such as the risk analyst presenting the result of a quantitative risk assessment to the decision-maker, we study how differences in the risk perspectives influence the exchange of information about risk between these actors. We try to identify some main challenges and barriers in the risk communication in the different situations.

TABLE 6.1 The different communication scenarios discussed, with an indication of which actors are involved (marked with an x) (based on Veland and Aven 2013)

Actor Scenario	Decision-maker	Risk analyst	Expert	Laypeople
1. A risk analyst presenting the result of a quantitative risk assessment to a decision-maker	x	x		
2. An expert providing risk-related input about the occurrence of a specific type of event to a risk analyst		x	x	
3. A risk analyst presenting the result of a risk assessment to laypeople		x		x
4. A decision-maker communicating with laypeople on a risk-related issue	X			x

Discussion on how the risk perspectives influence the risk communication

The issue to discuss is how the risk perspectives, based on the five views on risk defined above, influence the risk communication between the four actors defined: decision-makers, risk analysts, experts and laypeople. The discussion is based on a set of scenarios, as shown in Table 6.1. For each scenario, we will discuss possible communication problems and barriers resulting from the risk perspectives of the involved actors. Where appropriate, we will also reflect on ways the actors can reduce these negative effects.

In the following, we look more closely into these four scenarios, linking them to the relevant actors and their risk perspectives.

Scenario 1: A risk analyst presenting the result to a decision-maker

Let us start with the not uncommon situation that both actors have a chaotic view. Fundamental concepts like probability, uncertainty and risk are not properly understood, and no scientific foundation is present that can provide proper interpretations of the quantities presented. Clearly the situation would lead to poor communication. The analyst will fail in transmitting his/her message to the decision-maker. The results from the analysis include a number of probabilities and expected values, but, without clear and easily understandable interpretations, it will not be possible for the decision-maker to appreciate the meaning of these figures. If the analyst refers to an assigned probability equal to 0.2 (say), the meaning of this number must be explained in a way that is comprehensible, and if the risk perspective of the

analyst is a chaotic one, he/she is not able to do this. Another aspect is the context in which the numbers are produced. What are the assumptions on which the assessment results are based? With a chaotic view, the analyst can produce formulas and numbers but hardly any meaningful comments and reflections on the tool used to describe the risk, which would be essential for the decision-maker to fully understand the quantitative analysis carried out and place the result in its correct context, taking into account the limitations and boundaries of the assessment. If the decision-maker has a chaotic view, he/she is not able to ask for the key information required to support the decision-making. The lack of conceptual precision would in practice lead to a completely meaningless communication between these two actors.

Now, suppose that the decision-maker still has a chaotic view, but the risk analyst has one of the perspectives 1–3. This is a common situation in real life, as the analysts are trained as risk analysts and consequently have some background in the scientific pillars of the risk field, whereas the decision-maker normally lacks such training. The analyst is aware of the fact that the decision-maker lacks competence in the risk field and may seek to meet this challenge by trying to keep things simple and avoiding discussions of uncertainties (Aven 2011b, p. 125). However, in this way, risk could be poorly described, as uncertainty is an important dimension of all the risk perspectives. Even if the decision-maker lacks fundamental training in risk, the risk communication can be informative, provided that the analyst does his/her job in a professional way. Managers and politicians are able to relate to and deal with uncertainties and risk; these tasks are largely what their job is all about – to make decisions under uncertainty and risks. Managers are usually well-equipped people, who will quickly understand what is at stake and what the key issues are, if the professionals can do their job. The problem is, rather, that the analysts are not able to report the uncertainties and present them in an adequate way.

Next, suppose that the decision-maker has the 'objective view', whereas the analyst has either the 'uncertainty view' or the 'non-probabilistic view'. Problems can then easily arise, as the decision-maker is expecting to see some objective results – the truth about risk – whereas the analyst presents a subjective risk-uncertainty description. In this case, there is a need for a thorough process to make the decision-maker understand and acknowledge the analyst's perspective. Strong arguments for adopting such a perspective are then clearly required, to convince the decision-maker to give weight to the results and use them in the decision-making process.

Finally, let us consider the situation in which the analyst has the 'non-probabilistic view' and the decision-maker the 'uncertainty view'. Here, the communication could be challenging, as the decision-maker is not familiar with the non-probabilistic methods, and the presentation of these alternative

ideas is not done in a way that makes it possible to fully appreciate their meaning (based on the author's experience, these are common situations in real life). The decision-maker may find that the analyst addresses some relevant and interesting points, but, as the presentation of these ideas is so poor, he/she may be reluctant to give weight to the findings.

Scenario 2: An expert providing risk-related input to a risk analyst

Now, we study scenario 2: an expert providing risk-related input to a risk analyst. Let us first consider a situation in which the expert has a 'chaotic' view on risk and the risk analyst has one of the scientifically founded perspectives, 1–3. In this situation, the risk analyst is equipped with precise concepts and tools to understand and systemize risk, which can be used as a guide for dealing with the input given by the expert. This does not necessarily mean that the communication between the expert and the risk analyst will be unproblematic. If, for example, the risk analyst has an objective interpretation of risk (risk perspective 1 or 3), the expert can experience the risk analyst as being too narrow-minded, because of the extensive use of frequency-based probabilities in the analysis. This can create resentment from the expert, because of the scope of the input requested by the risk analyst. If, on the other hand, the risk analyst has a risk perspective in which uncertainty is the main component (risk perspective 2), the view on risk is wider, and input about underlying assumptions and limitations is considered to be equally important. In this case, it is reasonable to believe that an expert with a chaotic risk perspective will bear less resentment towards the risk analyst. However, in this case, problems may also occur in the risk communication, as the expert has difficulties in understanding the concepts used by the analysts, for example knowledge-based probabilities.

Next, suppose that the expert has an 'objective view' on risk and the risk analyst has an 'uncertainty'-based risk perspective. In this case, the expert has a scientifically founded perspective on risk, based on the assumption that an objective, true risk exists. This situation could quickly lead to a discussion on fundamental issues about how to understand and describe risk and the use of different types of probabilities. The expert would like to estimate the true risk (frequentist probabilities), whereas the analyst is concerned with describing uncertainties (typically using knowledge-based probabilities). From the analyst's point of view, the differences in underlying perspectives need not be a problem in the communication, as long as the experts provide the information that the analyst needs: probability assignments and the knowledge and assumptions that they are based on. These assignments can be elicited by asking for frequency type of judgements, for example: in the case of 100

similar situations, for how many would you predict that the event of interest would occur? From this judgement, a knowledge-based probability can be assigned, but the experts need not use or refer to such probabilities themselves. This would not resolve the differences in perspectives but would meet the information required by the analysts. It is likely then that the experts would agree to provide input to the analyst, if the communication about the overall approach and thinking is made clear by the analyst. The expert may not agree on the suitability of the analyst's perspective but has no problem in providing the input asked for.

We can make similar arguments for the case in which the expert has an 'objective view' on risk and the risk analyst has a 'non-probabilistic'-based risk perspective. Here, both actors believe in an objective risk, but the expert may not be familiar with the non-probabilistic methods to describe the epistemic uncertainties. Hence, the analyst needs to put a lot of energy into explaining the relevant concepts and requesting information in a format that is suitable for the experts.

Scenario 3: A risk analyst presenting results to laypeople

Next, we study scenario 3: a risk analyst presenting the results of a risk assessment to laypeople. First, suppose that both the risk analyst and the laypeople have a 'chaotic view' on risk. This would mean that the results from the risk assessment presented by the risk analyst would have no scientific foundation and, thus, lack precision and consistency. In such a situation, public scrutiny would most likely identify and emphasize weaknesses in the methodology and results. The risk analyst would fail to provide a credible response to this criticism, because of the 'chaotic view' on risk that the risk assessment is built on. Further, criticism from laypeople founded on a 'chaotic view' on risk would result in a rather meaningless communication between the two actors. In the end, the laypeople would not trust the risk analyst. Low levels of confidence and trust between the actors represent a core barrier to establishing a common understanding of risk between them.

Now, let us assume that the risk analyst has adopted the 'objective risk view', while the laypeople have the 'risk=perception view' on risk. This situation was typical in the 1970s and 1980s, for example in relation to nuclear power plants, when the risk analysts tried to convince laypeople that this industry is safe (having low and acceptable risk). Similar situations are also common today (Aven 2011c). The results presented describe the risk analyst's estimate of the 'true' risk level, represented by frequentist probabilities, based on past experiences and knowledge. The risk perceptions of the laypeople are shaped by the beliefs and conceptions of individuals and groups and can be further amplified or attenuated by social processes in society (Kasperson et al. 1988). A typical communication barrier in this

situation is that laypeople question the basis on which the results are built, for example conditions not included in the risk assessment or assumptions not adequately reflecting the present situation or the future. Another barrier is the analysts' use of criteria expressing that risk is acceptable by reference to low computed probabilities. This type of argumentation cannot be justified, as risk is more than probabilities (refer to Section 4.2) and laypeople also protest against it. Risk communication on this basis could lead to public criticism, which in its turn could amplify the laypeople's concerns and, thus, increase the barrier to communication and risk understanding between the two actors.

Let us now consider a situation in which the risk analyst has an 'uncertainty view' on risk and the laypeople still have a 'risk=perception view'. The risk assessment could still be largely based on probabilities, but the uncertainties are given more weight. With an 'uncertainty view', a broader risk picture is produced, reflecting the knowledge and the lack of knowledge on which the probabilistic analysis is based. Laypeople could question the quality of the analyses and their results, as they are not used to expert reports which do not provide clear answers. There seems to be growing understanding among people that things are complex and uncertainty is an issue we cannot ignore. People are faced with uncertainties in relation to potential pandemics, in relation to terrorist attacks, etc. They will understand that there are no numbers that can fully describe the risk in such situations, provided the analysts and experts do their job properly, i.e. establish a strong scientific platform for their thinking and the communication on the risk and uncertainties. Creating trust among laypeople is difficult but is certainly dependent on the analysts' and experts' ability to talk about the risk and uncertainties in the right way. Unfortunately, such a platform is not always established.

Scenario 4: A decision-maker communicating with laypeople

Finally, we look into scenario 4: a decision-maker communicating with laypeople on a risk-related issue. There are many similarities between this scenario and scenario 3. The main difference is that, for scenario 3, the communication from the risk analyst is limited to the results from the risk assessment, while, in scenario 4, the decision-maker has a broader view on risk, where values could also play an important role in the communication.

Let us first consider a situation in which the decision-maker has an 'objective' perspective and the laypeople either a 'chaotic' or a 'risk=perception' view on risk. The decision-maker could now be inclined to mainly emphasize the results from the risk assessment in the communication, because of an underlying belief that the results provide the best available measure on the

'true' risk level. The 'true' risk level could thus be presented to the laypeople as the main argument for making a decision on the risk-related issue, and other aspects could be downgraded or left out in the communication. The likely response from the layperson could range between the two extremes of either trusting the decision-maker for making firm and reliable statements or showing a total lack of faith in the decision-maker, due to the missing concern for wider aspects related to the risk issue. The acceptable risk issue in relation to nuclear power is, again, a good illustration of the scenario.

Let us now consider the situation in which the decision-maker has an 'uncertainty view' on risk and the laypeople have a 'chaotic view' or 'risk=perception view'. What was said above for scenario 3 is also to a large extent relevant here, but the value issue has some interesting implications. Too great a focus on uncertainties could weaken the conclusions that the decision-makers would like to make, and they could be tempted to conceal the uncertainties or argue that they should not be given much weight. It is obvious that it could be challenging for the decision-makers to adopt this perspective in many cases, as the focus on the uncertainties means that they cannot easily communicate with strength that a solution is really safe.

Conclusions

In this discussion, we have defined five perspectives on risk and four risk communication scenarios, based on commonly found real situations. By assigning different risk perspectives to the risk actors in each of these four scenarios, we have demonstrated the possible effects that differences in risk perspectives can have on the risk communication between them. The above analysis shows that differences in risk perspectives can lead to serious problems and barriers in the risk communication. Table 6.2 presents the main findings of the analysis.

A key finding of this analysis is that the risk communication can be seriously hampered if the risk assessment and management lack a proper scientific platform. On the other hand, if a solid platform is in place, it is much more likely that the risk communication will work effectively, as the premises for the dialogue are clear. The main barriers to good risk communication are not the laypeople's poor understanding of the risks and the risk assessment tools, but the risk analysts who have not done their job in a professional way and established some scientific pillars for their work. In this book, arguments are provided for using the uncertainty view, as it is very general and founded on a logical dichotomy: between the risk concept, which is based on uncertainties, and the way risk is measured or described, in which the probabilities and other representations of uncertainties come into play. However, which perspective is to be preferred is not the issue in relation the discussion in this section. Independent of the perspective adopted, the requirement for

TABLE 6.2 An overview of the main findings of our analysis

Scenario	Observation 1	Observation 2	Observation 3	Observation 4
1. A risk analyst presenting the result to a decision-maker	If both actors have a chaotic view, the risk communication is meaningless	If the decision-maker has a chaotic view but the risk analyst has one of the perspectives 1–3, risk communication can be informative, provided the analyst is able to adequately report and communicate the probabilities and uncertainties	If the decision-maker has an objective view and the analyst either an uncertainty or non-probabilistic view, problems arise, as the decision-maker is expecting to see objective results	If the analyst has the non-probabilistic view and the decision-maker the uncertainty view, the decision-maker may find it difficult to appreciate the results, as he/she is unfamiliar with the non-probabilistic methods and how the results are presented
Suggested improvement measures	The risk analyst needs to establish a scientifically based risk perspective	The risk analyst needs to develop a risk communication scheme, which is based on a clear understanding of the meaning of the probabilities and the uncertainties	There is a need for a communication process to make the decision-maker understand and acknowledge the analyst's perspective	There is a need for a communication process to make the decision-maker understand and acknowledge the analyst's perspective. Considerable effort may be required, as the non-probabilistic view could be challenging to understand
2. An expert providing risk-related input to a risk analyst	If the expert has a chaotic view and the risk analyst an objective view, the expert can experience the risk analyst as being narrow-minded	If the expert has an objective view and the risk analyst an uncertainty-based risk view, this could lead to a discussion on fundamental issues about how to understand and describe risk	If the expert has an objective view and the analyst a non-probabilistic view, severe communication problems may occur, as the expert may not be familiar with the non-probabilistic methods and their rationale	
Suggested improvement measures	The analyst needs to explain relevant concepts and request information in a suitable format	The analyst needs to clearly communicate to the expert the overall approach and thinking, so that the expert can provide input in the format required	The analyst needs to explain relevant concepts and request information in a suitable format	

(continued)

TABLE 6.2 *(continued)*

Scenario	Observation 1	Observation 2	Observation 3	Observation 4
3. A risk analyst presenting results to laypeople	If both have a chaotic view on risk, communication would be meaningless – the analyst would fail to provide a credible response to public criticism	If the risk analyst has an objective view and the laypeople a risk-perception risk view, laypeople will question the basis that the results are built upon and disagree if the objective results are used to conclude on risk acceptability	If the risk analyst has an uncertainty view and the laypeople a risk-perception risk view, a broad risk picture is presented reflecting the knowledge and lack of knowledge, which could make laypeople question the quality of the analyses	
Suggested improvement measures	The risk analyst needs to establish a scientifically based risk perspective	The risk analyst needs to provide meaningful responses to public criticism, which acknowledge the difference between the underlying risk and its estimate with associated uncertainties, in order to gain the trust of laypeople	The risk analyst needs to clearly establish and communicate a strong scientific platform for his/her thinking, to gain the trust of laypeople	
4. A decision-maker communicating with laypeople	If both have a chaotic view on risk, communication would be meaningless – the decision-maker would fail to provide a credible response to public criticism	If the decision-maker has an objective view and the laypeople a chaotic or risk- perception view on risk, the likely response from the laypeople could range from full trust to a total lack of faith in the decision-maker	If the risk analyst has an uncertainty view and the laypeople a chaotic or risk- perception view on risk, too much focus on uncertainties could weaken the conclusions that the decision-maker would like to make	
Suggested improvement measures	The decision-maker needs to establish a scientifically based risk perspective	The decision-maker needs to acknowledge the difference between the underlying risk and its estimate with associated uncertainties, in order to gain the trust of laypeople	The decision-maker should be honest about the involved uncertainties and strive for a balanced characterization of the uncertainties	

professionalism in relation to the scientific platform is the key. If a concept is introduced, it must be given a meaningful definition and interpretation. That is unfortunately not the case today in many situations (e.g. Aven 2012a). The objective view faces problems other than, for example, the uncertainty view but, even for the objective perspective, meaningful communication can be obtained if due consideration is given to the understanding of the concepts introduced and the uncertainties involved. There has been a tendency for risk analysts and decision-makers coming from the objective perspective to conceal uncertainties, and we see that this is still often the case (e.g. Aven 2011c). On the other hand, in following the uncertainty view, we may experience the other extreme: that too great a focus is placed on the uncertainties. What is the proper level is for the risk assessment discipline to decide, through the establishment of proper scientific principles and methods, as presented in the present book. More research is required on this issue, but equally important is the recognition among risk professionals that meaningful risk communication relies on a solid scientific basis. Improvements must be made in this area to bring forward risk analysts and also decision-makers that have the necessary competence and understanding for these matters.

6.2.3 The dilemma between being authoritative and open/transparent

History has shown that authorities and governments are not always open and transparent about their understanding of the nature of risks to the public and about the process they follow in handling them. Two illustrations are the so-called 'mad cow disease' (Creutzfeldt-Jakob disease) in the UK in the late 1990s (Powell and Leiss 1997) and the nuclear risk in the 1970s and 1980s (HMSO 1988). The perspective taken was that the risks were well managed by private companies and public regulatory authorities and were essentially negligible. The uncertainties were not properly acknowledged or communicated. Such a 'we know best' strategy led straight to the lack of trust in the authorities that many agencies and risk management institutions face today. Most people assume that the authorities try to balance different concerns and interests and like to avoid 'unnecessary' stress and panic. That is one reason for their suspicion, if the authorities pursue a typically paternalistic style of risk management and regulation. The authorities will lose public trust and lack credibility when they justify their decisions. We also observed this effect in relation to the swine flu vaccine (Rubin et al. 2010). Public authorities said little about the potential negative side effects of vaccination, in order not to worry the public. It was exactly this attitude, however, that created public outrage in many countries.

The authorities are of course faced with a dilemma. Although openness and transparency are in general desirable, their uncritical use can have severe

negative effects, such as stress and panic in huge populations. Yet, empirical research has demonstrated that open information about potential threats has very rarely resulted in panic or over-cautious behaviour (Helsloot and Ruitenberg 2004, Quarantelli 1993). On the contrary, when information is withheld and then suddenly released by third parties, panic reactions are more likely to occur. Given the overwhelming evidence in this issue, a policy of openness and transparency should be endorsed and practised. It helps people to be aware of the risks that they face and, in the long run, to build trust in the authorities.

People today seek the best information available. Public authorities should take a leading role, not camouflage their knowledge. The challenge is to develop a professional language and terminology that makes this communication work effectively. Current practice is not sufficiently developed to characterize and communicate risk and uncertainties in a way that different target audiences can make sense of and act accordingly. Public authorities need to invest extra effort not only to make information available to the general public (by placing it on a more or less open web account) but also to initiate communication programmes for each of the relevant stakeholders and target audiences. A huge challenge for authorities is to make scientific and professional reports comprehensible for the public. The transformation process may easily lead to biases – at least for one party in the debate. It is not sufficient to refer to probabilities – it is also necessary to say something about the knowledge base on which these are founded. If we think again about the swine flu example, a balanced way of expressing the risk would be to say:

> The vaccine could have unknown side effects. Some of them are known and we can control them, others are not and we do what we can to investigate and monitor them. We think it is unlikely that severe side effects will occur, but the knowledge base is rather weak and we cannot exclude the possibility.
>
> (Aven 2015b)

What is balanced can of course be discussed. In Aven and Renn (2018) it is mentioned that one of the reviewers of that paper commented that the parents of a child who developed narcolepsy as a consequence of the vaccination would probably not call this expression of risk balanced – they are now suing the government for damages. As a response, Aven and Renn comment that the authorities did not present risk in this way. Rather, the typical format was to ignore the risks related to potential side effects. Using a risk expression as above, the many relevant aspects of risk have been revealed, in a way which is considered rather balanced.

We know that many people have problems in understanding and acknowledging uncertainties: as long as there is a possibility, the event is considered bound to happen. We need better methods and processes that help people to gain a balanced perspective on risks, uncertainties and probabilities. Examples are needed from real life, showing that we live perfectly well with risks and uncertainties – for example in relation to traffic. We need to be crystal clear what a probability means, for example, when stating that there is a specific probability of the event occurring. The current nomenclature, as used in practice, is not good enough for effective communication. We rarely hear authority officials providing clear interpretations of probabilities. How can we then obtain successful communication with the public?

The main lesson for risk managers and regulators is that transparency and openness are essential for gaining trust and confidence. Sometimes, such openness is not well understood, and information may be taken by a special interest group to serve their specific interests and to mobilize public outrage. Withholding information, however, is not an adequate solution for avoiding this. On the contrary, if this strategy becomes known to the public, one can expect an explosion of outrage and accusations. Rather than trying to filter information, public authorities should concentrate on methods of how to best communicate risk information and how to engage stakeholders and the public in constructive risk management dialogues. Many risk communication guidebooks and public involvement manuals have been published that provide valuable guidance to the authorities. There seems, however, to be a reluctance to pursue this path and to follow this advice. With the exception of proprietary information and information that may damage public security (for example, strategies against terrorism), an open and transparent information policy is recommended.

See also the discussion in Section 8.2.

7 Risk management and governance

This chapter addresses some fundamental issues related to risk management and governance. First, in Section 7.1, we highlight some overall principles of risk management and governance. Then, in Section 7.2, we review basic theory related to cost-benefit type of analysis. Section 7.3 looks more closely into the cautionary and precautionary principles and the related robustness and resilience-based strategies. Section 7.4 discusses the call for a shift from risk to resilience, as was briefly introduced in Section 1.5. Then, in Section 7.5, we review fundamental principles for improving governmental policies on risk. Finally, Section 7.6 discusses some foundational issues related to risk governance and different types of risks.

7.1 FUNDAMENTAL PRINCIPLES OF RISK MANAGEMENT AND GOVERNANCE

Current knowledge about risk management and governance can be summarized in the principles presented in Section 3.1.1 (items 19–24). Three major strategies are needed for managing or governing risk: risk-informed strategies (I), cautionary/precautionary/robustness/resilience strategies (meeting uncertainties and potential surprises) (II) and discursive strategies (III). The risk-informed strategy refers to the treatment of risk – avoidance, reduction, transfer and retention – using risk assessments in an absolute or relative way. The cautionary/precautionary strategy highlights features like containment, the development of substitutes, safety factors, redundancy in designing safety devices, as well as the strengthening of the immune system, diversification, design of systems with flexible response options and the improvement of conditions for emergency management and system adaptation. An important aspect here is the ability to adequately read signals and the precursors

of serious events. All risk regulations are based on some level of such principles to meet the uncertainties, risks and the potential for surprises. The discursive strategy uses measures to build confidence and trustworthiness, through the reduction of uncertainties and ambiguities, clarification of facts, involvement of affected people, deliberation and accountability (Renn 2008, SRA 2015b).

In addition to these strategies it is also common to refer to 'risk-based requirement' strategies based on the use of codes and specific requirements that need to be met (ISO 2016, Aven and Kristensen 2019), applicable when the situations considered are simple – the phenomena and processes considered are well-understood and accurate predictions can be made. An example is today's specific requirements used for how to design and operate safety (barrier) systems in the petroleum industry, which are founded on many years of experience with extensive use of risk assessments. If these requirements are met, no further risk assessments are required for the hazards and safety systems covered by the requirements. The basic strategies I and II have largely been replaced by a 'risk-based requirement' strategy. However, when new technical concepts and arrangements are introduced, for instance when moving the control rooms from offshore installations to office buildings onshore, a more traditional risk assessment strategy, combined with a robustness/resilience strategy, is required (Aven and Kristensen 2019).

Risk management is to a large extent about balancing development and protection. Different principles, strategies and tools give different weights to these two main concerns; see Figure 7.1. Protection is supported by the cautionary and precautionary principles and related measures that can improve the robustness and resilience of relevant systems. Development, on the other hand, is promoted by cost-benefit type of analysis, as these tools are expected value based and, hence, give little weight to uncertainties and risks.

The risk assessments provide decision support for obtaining this balance, more specifically in relation to choosing between alternatives, the acceptance of activities and products, the implementation of risk-reducing measures, etc. The generation of the risk information is often supplemented with decision analysis tools such as cost-benefit analysis, cost-effectiveness analysis and multi-attribute analysis. All these methods are systematic approaches for organizing the pros and cons of a decision alternative, but they differ with respect to the extent to which one is willing to make the factors in the problem explicitly comparable. Independent of the tool, there is always a need for a managerial review and judgement, which sees beyond the results of the analysis and adds considerations linked to the knowledge and lack of knowledge on which the assessments are based, as well as issues not captured by the analysis.

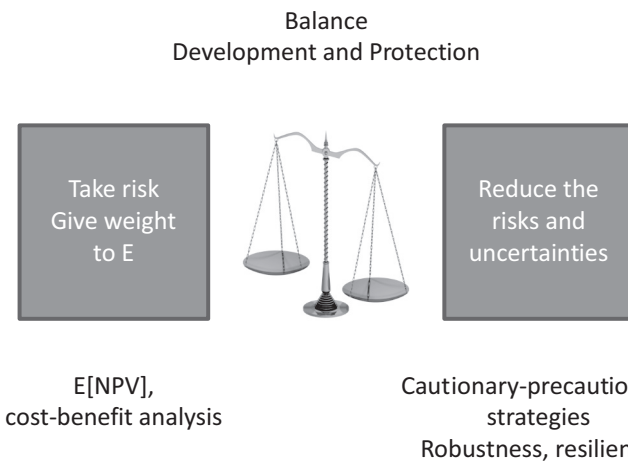


FIGURE 7.1 Risk management as a balancing act. E: Expected value (based on Aven 2014b, 2017b)

7.1.1 Risk acceptance criteria and tolerability limits

In risk management, it is common to introduce constraints, in particular related to safety aspects, to simplify the overall judgements and ensure some minimum performance level on specific areas, to avoid the consideration of too many variables at the same time. Such constraints are often referred to as risk criteria, risk acceptance criteria and tolerability criteria; see e.g. Rodrigues et al. (2014) and Vanem (2012). For example, in Norway, the petroleum regulations state that the operator has a duty to formulate risk acceptance criteria relating to major accidents and to the environment. This practice is in line with the internal control principle, which states that the operator has full responsibility for identifying the hazards and seeing that they are controlled. This practice is, however, debated, and in a recent paper Abrahamsen and Aven (2012) argue that it should be reconsidered. It is shown that if risk acceptance criteria are to be introduced as a risk management tool, they should be formulated by the authorities, as is the common practice in many countries and industries, for example in the UK. Risk acceptance criteria formulated by the industry would not serve the interests of the society as a whole. The main reason is that an operator's activity usually will cause negative externalities to society (an externality is an economically significant effect, due to the activities of an agent/firm, that does not influence the agent's/firm's production, but which influences other agents' decisions). The increased losses experienced encourage society to adopt stricter risk acceptance criteria than those an operator finds optimal in its own interest.

The criticism of the use of such criteria also covers other aspects; see e.g. Aven (2015a). First, tolerability or acceptance levels expressed through probability ignore important aspects of risk, as discussed in Section 4.2. A key point is that the strength of knowledge on which the probability judgements are based is not reflected in the probabilities used for comparing with these levels. Secondly, the use of such criteria can easily lead to the wrong focus: namely, meeting the criteria rather than finding the best possible solutions and measures, taking into account the limitations of the analysis, uncertainties not reflected by the analysis and other concerns important for the decision-making. As strongly highlighted by the risk analysis science (see also Apostolakis 2004), a risk decision should be risk-informed, not risk-based. There is always a need for managerial review and judgement.

7.1.2 The risk management process

The risk management process can be broken down into the following steps (in line with what one finds in standards such as ISO 31000 and most risk analysis textbooks (e.g. Meyer and Reniers 2013, Aven 2015a):

i. Establish context, which means, for example, to define the purpose of the risk management activities and specify goals and criteria.
ii. Identify situations and events (hazards/threats/opportunities) that can affect the activity considered and objectives defined. Many methods have been developed for this task, including checklists, HAZOP and FMEA.
iii. Conduct cause and consequences analysis of these events, using techniques such as fault tree analysis, event tree analysis and Bayesian networks.
iv. Make judgements of the likelihood of the events and their consequences and establish a risk description or characterization.
v. Evaluate risk, to judge the significance of the risk.
vi. Risk treatment.

In addition, implementation issues related to the risk management process need to be mentioned, such as leadership and commitment; see, for example, ISO (2018), Banks and Dunn (2003) and Teng et al. (2012, 2013).

Risk management is closely related to policy and policy analysis. A policy can be defined as a principle or plan to guide decisions and achieve desirable outcomes, and the term applies to international organizations, governments, private sector organizations and groups, as well as individuals. For example, when lawmakers pass legislation on safety for workers, this is a public policy decision, whose aim is to protect the rights of workers within

the society. The development and operation of policies are often structured by the following stages, inspired by decision theory (e.g. Althaus et al. 2018):

1. Problem identification – the recognition of an issue that demands further attention
2. Generating alternatives, analysis
3. Processing covering aspects like policy instrumentation development, consulting, deliberation and coordination
4. Decision-making
5. Implementation
6. Evaluation (assessing the effectiveness of the policy)

Linking stage 6 with 1, the process is referred to as the policy cycle. It has similar elements to those found in the quality and project management field for ensuring continuous improvement – plan, do, study and act. The above steps i–vi for the risk analysis process can also be structured in line with this cycle. The risk field provides input to the elements of the policy process, for example by:

- Conceptualization and characterization of the problem/issue, covering aspects like objectives, criteria, risk, uncertainties, knowledge and priorities.
- Structuring the problem, by clarifying and highlighting key principles (e.g. the precautionary principle) and dilemmas, such as the balance between development and value creation, on one side, and protection, on the other.
- Statistical data analysis to identify those hazards/threats that contribute the most to risk, and in this way guide the decision-making on where to most effectively reduce the risk.
- Risk assessments and in particular Quantified Risk Assessment (QRA) of alternative potential developments (for example, technological arrangements and systems), to be able to compare the risk for these alternatives and relate them to possible criteria and other concerns such as costs.
- Risk perception and related studies, providing insights into how different actors perceive the risk and what concerns they have regarding the risk and the potential consequences.

7.2 COST-BENEFIT TYPE OF ANALYSIS

Risk assessments are conducted to understand and characterize risk and in this way support decision-making on the choice of alternatives and measures. The risk assessments provide input to decision analysis tools and

particularly cost-benefit analysis (CBA). In risk management contexts, CBA is widely used. The advantage is that a simple approach is produced for comparing alternatives, and it is commonly believed that the analysis leads to cost-effective solutions in a wide sense.

Following a traditional cost-benefit analysis, the benefits and costs of a project (decision alternative) are expressed in money. In practice, it is easy to transform market goods to monetary values, since the prices of the market goods correspond to the society's willingness to pay (WTP). It is, however, more difficult to determine the WTP for non-market goods, and different methods are used, including contingent valuation and hedonic price techniques (Hanley and Spash 1993). In practice, the expected net present value, NPV, is computed as a basis for making a judgement of which alternative to choose. The formula used to calculate NPV is:

$$NPV = \sum_{t=0}^{T} \frac{X_t}{(1+r_t)^t}$$

where T is the time period considered (normally expressed in years), X_t is equal to the cash flow at year t, and r_t is the required rate of return, or the discount rate, at year t, t = 0,1,2, . . ., T. The cash flows are in general uncertain and are replaced by their expected values $E[X_t]$. The determination of the rate of return is based on the so-called Capital Asset Pricing Model (CAPM) (Copeland and Weston 1988). Using E[NPV], comparisons between alternatives can easily be conducted. A project (alternative) is considered attractive if the expected cost-benefit is positive, i.e. E[NPV] > 0.

Hence, the approach is based on the use of expected values. To see what that means and to simplify the discussion, consider a case where T=0, so time is not an issue, and $X = X_0$ can either take the value –1000 or 10, with probabilities of 0.001 and 0.999, respectively. We can think of the negative value as being the result of an accident and the positive as the benefit gained when this accident does not occur. Then, the expected value E[X] is equal to $-1000 \times 0.001 + 10 \times 0.999 \approx 9$. Hence, the expected value is positive, and the project is attractive: the benefits are considered larger than the costs.

In this formula, we can think of the -1000 value as being the result of multiplying the number of fatalities (given the accident) with the Value of a Statistical Life (VSL). The VSL is interpreted as the maximum value one is willing to pay to reduce the expected number of fatalities by 1.

From a risk management point of view, the potential loss of –1000 is a major concern. The expected value does not reveal the risk associated with X, which obviously would be important for the decision-making. In the extreme situation, the company could go bankrupt in the case of a big loss. In practice, there may also be issues related to the determination of the probabilities. What if the probabilities have been specified on the basis of

very poor background knowledge (they are seen as rather arbitrary)? Should not that affect the conclusions? Yes, it should, as 9 then has no strong basis.

Although this argumentation is somewhat crude and vague, we see that using the criterion E[X] as a basis for making the right decision is indeed problematic. Yet, there are arguments supporting the use of expected values in the decision-making. The idea is that we need to focus attention on a portfolio of many projects, not only one. Considering such a portfolio, the 'disturbance' from risk and uncertainties is reduced and basically eliminated in some cases, as justified by the law of large numbers.

From a practical point of view, the question is then: what are the conditions that make the use of an expected value based method such as E[NPV] suitable or not suitable? By being precise on the concepts discussed, from uncertainties and risk to probabilities and expected values, we seek to provide some answers.

7.2.1 The justification of using expected values, with discussion

To justify the use of expected values, we make use of the law of large numbers. Let us consider n activities of a specific type, and let the future values associated with these activities be denoted $X_1, X_2, \ldots X_n$. These values are assumed to be independent random variables with a common frequentist probability distribution G and related expected value μ. Hence $\mu = E_f[X] = \int x dG(x)$. According to the law of large numbers, the average value $\overline{X}$ of these n quantities would be approximately equal to μ when n is large. Hence, focus can be placed on the expected value μ, instead of on the actual quantity of interest, the value $\overline{X}$.

This analysis is a thought-constructed reality. The distributions and random variables exist in our heads to approximate reality. For some applications, these approximations would produce accurate results and, hence, justify the use of expected values to replace the actual quantities of interest $\overline{X}$. Think about health settings and traffic contexts, where we can have huge populations of similar units, and 'objective probability distributions' (I) can be produced; i.e. frequentist probability distributions can be meaningfully defined and accurate estimates derived. Thus, we need a lot of similar units, and the variation in values between them must be known. In such situations, we basically know the expected values, and, with a large population, these values would be approximately equal to the quantities of interest, the average values. The CBA approach is working.

The problems arise when we leave category I; we face uncertainties and allow for surprises in relation to the existing knowledge. In practice, such situations are common. A lot of systems and activities in today's world have

unique features, and the uncertainties are large. Many systems are complex – it is acknowledged that surprises will occur.

Can we still use CBA and expected value based analyses? Yes, we can, but we should use them with caution. They alone do not provide a clear answer regarding what decision to make.

When discussing this type of issues, it is essential to know what quantity is really of interest. Is it the health of one specific person, or is it the health of the whole population in the country? In the former case, specific information and knowledge about the person is essential, but this is not relevant in the latter case.

Consider a company running two projects which are quite unique, involving many developing features. For these projects, frequentist probabilities cannot be justified, as there is no meaningful way of defining an infinite population of similar projects. However, knowledge-based probabilities can be used to assess the future value of the projects. The analysts have some knowledge about the projects, but there are considerable uncertainties related to the values of these projects. Nevertheless, the average value $\bar{X}$ could be the key quantity of interest, but, in this situation, we do not have a direct link to the expected value E[X]. Clearly, if we choose to use E[X] alone to direct the decision-making, we may seriously misguide the decision-maker, as the expected value E[X] could be far away from the actual value $\bar{X}$. Consequently, there is a need for rethinking.

As another example, assume that we consider quite a few activities, and the values are either quite small positive or extremely large negative (which corresponds, for example, to a major accident). Also, in this case, the expected value approach leads to a problem, even in the situation that frequentist probabilities can be meaningfully defined and are known. The issue is again that the average value $\bar{X}$ could be far from $\mu = E_f[X]$, since the average value is likely to be a relatively low positive number or an extremely high negative number, if such an extreme event occurs. The case with knowledge-based probabilities or frequentist probabilities subject to large uncertainties adds another argument to seeing beyond the expected values. The knowledge supporting the probabilities could be weak, and the estimators of the frequentist probabilities could be poor. Again, the result is a potentially big gap between the average value $\bar{X}$ and the (estimated) expected value.

Let us illustrate the discussion with a more concrete example.

Lifeboat case

In the oil and gas industry in one country, the question addressed is whether or not to install more modern lifeboats on the offshore installations, to improve the safety in the case of major accidents. The number of installations is about 100. The costs are estimated as €2–5 billion. Determining the

expected number of saved lives is difficult, but any reasonable calculations of the expected cost per expected number of saved lives lead to very high numbers (ICAF, Implied Cost of Averting a Fatality), and the E[NPV] gives a clear message: the measure cannot be justified on the basis of expected value based thinking.

The problem is, however, that in this case expected value cannot be used as a criterion to determine whether this measure should be implemented or not. The expected value based metrics do not approximate well any average real quantity of interest. Rather, the issue is the possible occurrence of extreme events with low computed probabilities, and the measure then could be decisive for saving many people's lives in these situations. The measure will reduce the risk and uncertainties related to such extreme events. This benefit needs to be balanced against the costs of the measure, but not by multiplying probabilities and values, as risk acceptability and related decision-making de facto is not and should not be determined by such numbers alone. There is no tool that can prescribe what is the optimal decision in a case like this. It is a matter of balancing different concerns, a potential uncertain benefit against a cost. What is the proper decision also needs to be seen in a historical and social context.

Take the extreme case that the measure is about having lifeboats at all. In isolation, the cost-benefit analysis would easily lead to the conclusion that we do not need lifeboats, as the computed probability of an event requiring these boats is so small. However, such an attitude to risk would normally be unacceptable, as it leads to situations with no effective emergency preparedness systems in the case of a major accident. Safety and security measures are justified by their reference to risk and uncertainties, not to expected values. A major accident may happen; history has indeed shown that it can occur, and then measures need to be available to effectively save people. There will always be a need for trade-offs, balancing different concerns, but there is no rationale showing that expected values provide the key formula for making a good decision in such a case, as these values do not approximate well the quantities of interest.

CBA to support decision-making

Consider a measure to reduce the risk and uncertainties related to the possible occurrence of a major accident on one particular installation. As an example, think of an instance where a new type of risk assessment is implemented, which is believed to give better decision support. The effect of this measure on risk is difficult to quantify – on cost it is easier. Again, the use of a CBA based on expected values would easily lead to the conclusion that the measure is not justified, despite the fact that this new assessment could help to identify possible severe events in some cases. As in the previous

example, the expected value would not approximate well any real quantity of interest; consequently, it should not be used as a key source for guiding the decision-making.

Major accidents can be avoided

The rationale for using expected values is that this value provides an accurate estimate of some real quantity of interest, typically some average value for a large population of units. As the above discussion shows, there are many reasons why the expected values are not close to these quantities. One argument not explicitly mentioned is that, even if we expect that a major event will occur in a specific population or period of time, based on history and average performance, it may not happen. Good safety management could prevent the event from occurring. A major accident does not need to occur, despite the fact that there is a computed probability of that happening. The benefit of good safety management could be no major accident, which would then have a value different from the expected value, which incorporates contributions from the occurrence of such events.

ALARP principle

Consider the challenge of implementing the ALARP (As Low As Reasonably Practicable) principle. It states that, in general, a measure that can improve safety shall be implemented, unless it can be demonstrated that the costs are in gross disproportion to the benefits gained. To verify ALARP, it is common to use cost-benefit analysis based on expected values. Can this practice be justified, in view of the above discussion?

Safety work aims at preventing accidents from occurring and people from being killed or injured and at reducing the related risks. The ALARP principle is implemented to support the safety work and obtain such a risk reduction. However, if expected values and cost-benefit type of analyses are used to guide the decision-making, and in particular what is ALARP, the risk is not really captured, as the expected value could be a poor risk metric.

Only in the case that we have many similar projects, and the variation in projects is known and not too large, can the practice be justified. This means that we basically have to ignore the potential for surprise, which is an important aspect of risk.

In general, when considering risk reduction and seeking to meet the ALARP principle, the following procedure is recommended (Aven and Flage 2018, Aven and Vinnem 2007):

1. If the costs are small, implement the measure if it is considered to have a positive effect in relation to relevant objectives or other reference values.

2. If the costs are large, make an assessment of all relevant pros and cons of the measure. If the expected present value (or similar indices) can be meaningfully calculated, implement the measure, provided this value is positive.
3. Also, consider implementing the measure if it generates a considerable positive effect on the risk and/or other conditions, for example:
    - Reducing uncertainty or strengthening knowledge
    - Strengthening the robustness in the case of hazards/threats, and/or strengthening the resilience.

This procedure acknowledges the importance of fundamental safety principles, such as robustness and resilience, to meet uncertainties and potential surprises.

7.2.2 Conclusions

In situations of type I with many similar projects (objective frequentist probability distributions can be established), cost-benefit types of analyses using expected values provide strong decision support, as the relevant metrics approximate well real-life quantities. In other situations (II), this is not the case, and these types of analyses must be used with care. In situations of category II, a rationale for the use of CBA-based decision-making cannot be given. In this case, the analysis argues in general for a process as described above for the ALARP (1–3), in particular when safety or security types of measures are considered. In general, pros and cons need to be assessed and an evaluation made, leading to a decision, without the strict use of formulae to prescribe the decision.

There are several issues also related to time t and the interest rate. See discussions in, for example, Harrison (2010) and Ale et al. (2015, 2018).

7.3 CAUTIONARY AND PRECAUTIONARY PRINCIPLES: ROBUST AND RESILIENCE-BASED STRATEGIES

Few policies for risk management have created more controversy than the precautionary principle, and it is still being discussed; see for example Aven (2011b), Cox (2011), Sandin (1999), Sandin et al. (2002), Löfstedt (2003), Sundstein (2005), Peterson (2006, 2007), Renn (2008), Aldred (2013), Boyer-Kassem (2017). Two common interpretations are (SRA 2015a):

- a principle expressing that if the consequences of an activity could be serious and subject to scientific uncertainties then precautionary measures should be taken or the activity should not be carried out
- a principle expressing that regulatory actions may be taken in situations where potentially hazardous agents might induce harm to humans or the environment, even if conclusive evidence about the potential harmful effects is not (yet) available.

The principle has a rationale, as no method – quantitative risk analysis, cost-benefit analysis or decision theory – can prescribe what the best risk management policy is in the face of scientific uncertainties. The principle is to be seen as a guiding perspective for risk handling, a perspective which is considered expedient, prudent or advantageous. However, it does not provide precise guidance on when it is applicable, as the judgement of what constitutes scientific uncertainties is subject to value judgements. If, for example, the scientific uncertainty is related to the difficulty of establishing a prediction model for the consequences (Aven 2011b), subjective judgements are needed to decide when this is actually the case.

The precautionary principle as here defined is not a decision rule, which tells "decision-makers what to do, given what they believe about a particular problem and what they seek to achieve" (Peterson 2007). A guiding perspective for risk handling as used here is rejected by scholars like Peterson (2007), who writes:

> From an intellectual point of view, this is not good enough. The respectable way to discuss decision-making based on qualitative information is to use qualitative decision theory, which requires that we have one or more precise formulations of the decision rule. Essentially, we need a principle that tells us what to do and what not to do for each possible input of qualitative information. Until such a formulation of the precautionary principle is agreed on, it is normatively empty.
>
> (Peterson 2007)

But what does the phrase "From an intellectual point of view" really mean? The following discussion will demonstrate that attempts made to use such a decision rule formulation fail to capture the essence of what the principle aims to achieve.

Let us return to the concept of the decision rule as expressed by Peterson (2007). A key point here is the expression "given what they believe". Decision-makers may have beliefs about what can happen in the case of an activity and even express these using some types of likelihood judgements. However, to rely fully on these beliefs is to violate the idea of the cautionary principle.

With uncertainties about the consequences C, care needs to be shown in giving weight to beliefs and judgements about C, as these can be more or less strong and even erroneous. An assessor (which could be the decision-maker) may judge an event F to be more likely than G, but the decision-maker should not give much weight to this when the judgement is poorly founded. The actual outcomes may not be consistent with the likelihood judgements made.

Attempts have been made to show that the precautionary principle leads to inconsistencies when used as a decision rule (Peterson 2006, Stefánsson 2019). The problem is, however, that the conditions applied to ensure these results build on comparisons of likelihood judgements. One such condition states that "If one act is more likely to give rise to a fatal outcome than another, then the latter should be preferred to the former, given that both fatal outcomes are equally undesirable" (Peterson 2006). As commented above, such judgements cannot be justified in the case of large uncertainties.

Much of the debate on this principle is due to different understandings of the fundamentals of the risk field, for example related to risk and uncertainties. If one studies the above references, it is evident that the risk field needs a stronger conceptual unity. From the perspective of the present author, a key point is the difference between the cautionary and precautionary principles (Aven 2011b). The former principle is broader than the precautionary principle, stating that if the consequences of an activity could be serious and subject to uncertainties, then cautionary measures should be taken or the activity should not be carried out, i.e. faced with risk we should take action. This principle is used for all industries. For example, in the Norwegian oil and gas industry, there is a requirement that the living quarters of an installation should be protected by fireproof panels of a certain quality, for walls facing process and drilling areas. There are no scientific uncertainties in this case: the phenomena are well-understood; yet measures are implemented which can be seen as justified on the basis of the cautionary principle. One knows that such fires can occur and then people should be protected if they occur. Of course, the decision may not be so straightforward in other cases, if the costs are very large. A risk assessment could then provide useful decision support, and, in line with the ideas on risk described in Chapters 3–5, weights should also be placed on the uncertainties. At the final stage, the decision-makers need to find a balance between the costs and benefits gained, including the weight to be given to the cautionary principle. In the following, we look more closely into the cautionary principles as a perspective for guiding risk handling.

7.3.1 The scope of the cautionary principle – its link to risk

John has a nice house. He has implemented many measures to ensure that the probability of fire is very low. Yet he has purchased a fire insurance policy.

A fire could occur, and he will not take the risk of losing everything. He gives weight to the cautionary principle.

As another example of the use of the cautionary principle, consider the German decision to phase out their nuclear power plants by the end of 2022 (Ethik-Kommission 2011). This decision was made following the 2011 Fukushima nuclear disaster. There are risks related to both potential nuclear accidents and nuclear waste. Judgements were made that the risks are unacceptable. Half of the German Ethics Commission, which paved the way for the German phase-out decision, argued that "Nuclear energy is not acceptable because of its catastrophic potential, independent of the probability of large accidents occurring and also independent of its economic benefit to society" (Aven and Renn 2018). They can be said to have given very strong weight to the cautionary principle. The other half argued using a cost-benefit type of reasoning: other means of electricity generation were feasible with almost the same benefit as nuclear power but with less risk (Renn 2015). Weight is also given to the cautionary principle in this case, although the argumentation is different. In most cases in life, trade-offs between different concerns must be made, and the cautionary principle then must be balanced against other attributes like costs and value generation.

As a third example, think of a car in which the driver considers passing another car on a rather narrow road. The driver may abandon the passing or choose to carry it out, increasing concentration and awareness when passing the car. The driver gives weight to the cautionary principle.

As a guiding perspective for risk handling, there are several aspects that the cautionary principle seeks to highlight. First, it points to the need for actions when the consequences C can be extreme. Caution is needed when the potential for such Cs exists. Related uncertainty and likelihood judgements affect the degree of caution.

Secondly, the cautionary principle points to actions when the consequences are sensitive to how the activity is realized, as in the car example presented above. Lack of awareness can, for example, easily lead to severe consequences. The same type of argumentation can be used for the offshore and nuclear examples. These examples also illustrate a third aspect, captured by the saying 'better safe than sorry'. It is considered wise to be cautious, even when it does not seem necessary, to avoid problems, failures and losses later. If not being cautious, one may later regret it. If you go for a hike in the mountains, it is wise to have extra clothes, in case the weather should change. The calculated risk reduction of having living quarters protected by fireproof panels of a certain quality, for walls facing process and drilling areas, may be low but justified by references to the cautionary principle, as discussed above. A fire scenario threatening the living quarters may occur, and the specific requirements ensure a minimum protection level.

In statistics, there are two types of errors: false-negative and false-positive. In science, it is generally considered more important to avoid false positives than false negatives, as discussed, for example, by Peterson (2007). We will avoid concluding that a substance has a positive effect when that is not the case. This is in line with cautionary thinking. Without a strategy for avoiding false positives, the consequences could be serious. We (society) will not allow a new treatment, if we are not sufficiently confident that it works. The point of departure is that the treatment is not effective, and the producer must demonstrate that it has an effect. In this sense, the burden of proof is reversed. Society does not have to prove that the treatment does not work.

As the last and fifth aspect, the cautionary principle highlights the case of scientific uncertainties – in this case, the principle is referred to as the precautionary principle.

It is illustrative to relate the cautionary principle to risk, as discussed in Chapter 4: in its broadest sense, risk can be viewed as the combination of the consequences of an activity and related uncertainties, denoted (C,U), where C is the consequences of the activity considered and U the associated uncertainties (what will C be?). Describing or characterizing the risk, we are led to (C',Q,K), where C' are the specified consequences, Q a measure (in a wide sense) of uncertainty and K the knowledge supporting this measure. This representation of risk covers, as special cases, most other commonly used conceptualizations of risk. Without loss of generality, we can also write risk as (A,C,U), where A represents events (changes, hazards, threats, opportunities), which can lead to some consequences C. The risk characterization can then be reformulated as (A',C',Q,K).

From this basis, we see that the cautionary principle applies when risk is judged high in the following ways:

1. There is a potential for C values that are extreme.
2. There is a potential for serious C values if the activity is not cautiously executed – C is very sensitive to how the activity is run.
3. There is a potential for serious C values if something unlikely, surprising, or unforeseen should happen (for example, an event A not anticipated or a new type of event A).
4. Weak knowledge about the consequences C of a specific type of activity, for example, about the effect of the use of a specific drug. There is a potential for serious C values.
5. There is a potential for serious C values, and these are subject to scientific uncertainties.

Some of these criteria are closely linked and overlapping, as for example 4 and 5.

7.3.2 The rationale of the principle: Implications

The cautionary principle states that, if risk is high in the sense of 1–5, caution is in place: measures should be implemented, or the activity should not be realized. The principle provides guidance, it does not prescribe what to do. No risk management principle should prescribe what to do as discussed above, as there is always a gap between principle and action. In the face of risk with the potential for serious consequences, there is no formula or approach that can objectively produce the best decisions. Theories exist, like the expected utility theory, but they all have limitations in providing clear answers on what is the best decision. Consequently, the use of risk management principles is needed, to provide guidance on how to think and make good decisions. In relation to risk, there are two main types of concern: the need to create values, on the one hand, and protection, on the other. The cautionary principle is of the latter type. It gives weight to the uncertainties. It has a role in notifying people and society in relation to protection against potential hazards and threats with serious consequences. A principle highlighting value creation is the use of traditional cost-benefit type of analysis CBA (expected net present value calculations), as risk and uncertainties are here not given weight beyond expected values. Adopting one of these principles and ignoring the others would clearly lead to poor risk management. We need both categories of principles, as well as principles highlighting other concerns, particularly the need to obtain a balance between development and protection; refer to the discussion in Aven and Renn (2018) and Section 7.1.

Passive smoking

The case of smoking and passive smoking is an interesting one, in relation to this discussion. Recently, we have seen a trend for governments to ban public smoking, often following intense debate (Aven and Renn 2018); refer to Section 3.2. For example, in UK (2006), questions are asked about the evidence for such a ban: is the decision a disproportionate response to a relatively minor health concern? The basis is CBA type of reasoning. As discussed in Aven and Renn (2018), the analysis demonstrates a lack of understanding of the fundamental principles of risk management and governance, see also Section 7.5.3. The approach used does not give proper weight to the importance of people and their well-being and the health conditions of having a smoke-free environment. A ban may also contribute to a general reduction of smoking in society, having strong implications. Highlighting the cautionary principle would justify such a ban to protect people from involuntarily being exposed to the health-damaging activities of others and generally reduce the effects of smoking in society.

The CBA perspective

In society, there is a continuous 'battle' between development, on the one side, and protection, on the other. This battle is rooted in differences in values and priorities but also in scientific and analytical argumentations. For example, public administration is strongly guided by the use of cost-benefit type of analysis. Risk and uncertainty considerations are given little attention beyond expected values. The rationale is that the expectation will approximate well the average value when considering a large portfolio of activities or projects (Hanley and Spash 1993, Aven 2017b); refer to the discussion in Section 7.2. This means, for example, that the risk related to a major accident in a country is given quite little weight in traditional cost-benefit analysis (CBA), when taking a national or global perspective. As a result, traditional cost-benefit analysis would, for example, normally 'justify' nuclear industry in a country.

The protection concern

The cautionary principle has a role to play in relation to this type of consideration and management. A warning is in place – there is a potential for serious consequences and there are uncertainties. The development tools have spoken – now it is time for the protection side to highlight important aspects for the decision-makers to adequately balance the various concerns. The protection side also needs a scientific voice and justification, as

1) CBAs have strong limitations as a scientific tool – they do not adequately reflect risk and uncertainties;
2) CBAs favour development at the expense of protection.

The arguments for these assertions are well known, see Section 7.2, the key point being that the analysis is based on expected value. Let us look into an example, to further illustrate the discussion.

A country has about 100 installations of a special type, which all have the potential for a major accident, leading to a high number of fatalities. A risk assessment is conducted and the total probability of such an event in the next ten years is computed as 0.010. From the assessment, one such major event is expected in this period. A safety measure is considered for implementation. It is, however, not justified by reference to a cost-benefit analysis, as the expected benefit of the measure is calculated to be rather small. The costs are considered too large in comparison with this expected value. The basic rationale is that we should expect one such event in the period and the measure considered would not really change this conclusion.

However, the perspective taken is close to being deterministic and destiny-oriented. One such event does not need to happen. Safety and risk

management aim to avoid such accidents, and, if we succeed, the benefits are high – saving many lives. The value of the safety measure is not fully described by the expected number. The measure's value is mainly about confidence and beliefs that the measure can contribute to avoiding an occurrence of the accident.

Probabilities are commonly used for this purpose. Implementing the safety measure can, for example, result in a reduction in the accident probability estimate from 0.010 to 0.009, which shows that it is less likely that a major accident will occur. However, the difference is small and will not really make any difference to the decision-making problem. One major accident is still foreseen.

It is essential to acknowledge that probability and probabilistic analysis are just tools for supporting decision-making. These tools do not capture all aspects of importance for the decision-making, as thoroughly discussed in the literature (e.g. Flage et al. 2014) and also addressed in Section 4.2.

From probability to confidence

The full effect of a risk-reducing measure is not adequately described by reference to a probability number alone. A broader concept of 'confidence' is better able to reflect the total effect. This concept is based on probability judgements, as well as assessments of the knowledge supporting these judgements. For example, it matters a great deal whether the probability judgements are based on strong knowledge or weak knowledge. In these judgements, due considerations need to be given to potential surprises, although their risk contribution is per definition difficult to measure or describe. As resilience measures are to a large extent motivated by meeting potential surprises and the unforeseen, it is also a challenge to adequately characterize the effect of resilience measures. Surprising scenarios will occur in complex systems, and traditional risk management approaches using risk assessment struggle to provide suitable analysis perspectives and solutions to meet the risks (Turner and Pidgeon 1997, Hollnagel et al. 2006, Aven and Ylonen 2018). Measuring the benefit of investing in resilience is thus difficult. Such an investment can contribute to avoiding the occurrence of a major accident, although the effect on calculated probability and risk numbers could be relatively small.

To further illustrate the need to see beyond approaches based on calculations alone, think about an event A, for which a very low probability number is computed. The probability is judged so low that the occurrence of the event is basically ignored; refer to the discussion in Section 4.2.2 on surprises. Following this discussion, suppose the probability judgement is based on a specific assumption, and, given this assumption, the probability is judged to be negligible. Hence, if the event occurs, it will come as a surprise,

given the knowledge available. However, the assumption could be wrong and, clearly, with a different knowledge base, the probability could be judged high, and the occurrence of the event would not be seen as surprising. The cautionary principle highlights the need for:

a) Further checking of the assessments made: is the knowledge supporting the judgement strong enough? Could there be a potential for surprises relative to current knowledge?
b) The consideration of measures that could strengthen the robustness and resilience of the relevant systems, in case a surprising event should occur.

The assessors may consider the situation to be characterized by rather strong knowledge, yet the cautionary principle stimulates both better analysis and robust/resilient measures. The key point made is that the analysis could have limitations in accurately reflecting the real world, and surprises can occur relative to current knowledge. This justifies robustness and resilience-based measures, for example the implementation of safety barriers, different layers of protection, 'defence-in-depth', redundancy, diversification, the ALARP principle, etc. Current industry practice is based on this thinking and these types of measures – the cautionary principle is commonly adopted.

Whether the uncertainties are scientific or not is not really the interesting issue in relation to this example and many others. Think about cautionary measures implemented in airports all over the world. We do not know when an attack will occur, but, certainly, if no such measures had been implemented, extreme events would have been the result. The cautionary principle is applicable and has played a key role in the way this problem has been dealt with. The cautionary principle has not been specifically referred to – as it is not broadly known – but the above discussion has shown that it is in fact a main perspective adopted for handling the risk. Using the broader concept of the cautionary principle instead of the precautionary principle, we can avoid unnecessary discussion about what type of uncertainties we face, and focus can be placed on action and how to manage the risk. However, for some specific situations, it may be important to clarify whether the uncertainties are in fact scientific, so that the appropriate measures are taken. In relation to the approval of new products, the concept of scientific uncertainties is important, to ensure proper qualification processes. Clarifying when we face scientific uncertainties is also important, in relation to other contexts, such as climate change, when more knowledge and science can reduce the scientific uncertainties and, in this way, clarify the issues and better distinguish between discussions about uncertainties and discussions about values.

Adaptive measures

When the uncertainties are large, 'adaptive risk management' is also attractive: different decision options are assessed, one is chosen and observations are made, learning is achieved and adjustments made (Cox 2012, Aven 2013b). It can be seen as a way of implementing a cautionary approach. See Bjerga and Aven (2015) for an example of an adaptive risk assessment in line with the risk perspective used in this book. Bayesian frameworks are often referred to when implementing adaptive policies but are not easily adopted in the case of large uncertainties; see for example discussion in Aven and Bergman (2012).

7.3.3 Conclusions

In general, decision rules should not be used in risk management. There are always uncertainties present, and there is no objective best way to handle these. The best we can do is to be informed by analysis and science, and acknowledge that there is a gap between the evidence part and the decision, which is about how much weight we should give to the uncertainties and what are our values. Risk management principles, like the cautionary principle, provide guidance on how we should think in this process and what should be highlighted to protect something of value. There are different interests in most activities in life, and there is often a need to protect 'weak' parties. History shows us many examples of when protection has failed, with the result that numerous people have suffered and the environment has been damaged. The cautionary principle highlights protectional aspects and is balanced against principles that seek development and growth. Too much emphasis on caution would hamper innovation and new arrangements and solutions. Risk management gives proper weight to the cautionary principle and finds the right balance between development and protection. The cautionary principle includes the precautionary principle, which is invoked in the case of scientific uncertainties. For many types of situations, the cautionary principle is the appropriate concept, but, as discussed above, there are also situations where it is important to highlight that the uncertainties are scientific, and the precautionary principle is the one reflected.

Table 7.1 summarizes the different types of situations discussed in this Section 7.3, with specifications of relevant actions/instruments. Risk assessments provide decision support, but their value is limited in the case of scientific uncertainties. Robustness and resilience policies are of particular importance in the case of large uncertainties.

Robustness and resilience-based policies and strategies can be viewed as justified by the cautionary and precautionary principles. The concepts reflect the ability of a system or organization to maintain or regain a normal state

TABLE 7.1 Crude categories of situations, with associated risk management approaches and actions/instruments (Aven 2019c)

Situation of high risk	Approach	Actions/Instruments
Potential for serious consequences. Scientific uncertainties	Risk management. Weight given to the precautionary principle	Risk assessment informed (limited knowledge). Ban, prohibition and/or restrictions on activity. Robustness and resilience policies
Potential for serious consequences. Uncertainties	Risk management. Weight given to the Cautionary principle	Risk assessment informed. Ban, prohibition and/or restrictions on activity. Robustness and resilience policies
Other situations characterized by high risk	Risk management	Risk assessment informed

given a change, disturbance or stress. See for example discussion in Aven (2016a) and SRA (2015b). Robustness is often referred to as the antonym of vulnerability (SRA 2015a). If A denotes the change, we are concerned with how the system works or is able to work given the occurrence of A. Using the risk terminology introduced in Chapter 4, vulnerability can be viewed as risk given A, i.e. Vulnerability = (C,U|A), and the description of vulnerability takes the general form (C',Q,K|A); see Section 4.2. In this view, resilience can be considered an aspect of vulnerability. We will discuss resilience in more detail in Section 7.4.

7.4 THE CALL FOR A SHIFT FROM RISK TO RESILIENCE

In recent years, calls have been made for a shift from risk to resilience, largely motivated by the need to meet the effects of climate change. The basic idea is that we need to be prepared when threatening events occur, whether they are anticipated or unforeseen. This section questions the extent to which this call will have and should have implications for the risk field and science. Is the call based on a belief that this field and science should be replaced by resilience analysis and management, or is it more about priorities: more weight should be placed on improving resilience? It is argued that the only meaningful interpretation of the call is the latter. Resilience analysis and management is today an integrated part of the risk field and science, and risk analysis in a broad sense is needed to increase relevant knowledge, develop adequate policies and make the right decisions, balancing different concerns and using our limited resources in an effective way. See also

Section 1.5, which provides a background and motivation for the discussion in this Section 7.4.

7.4.1 Delineating the risk and resilience fields and sciences

To simplify the nomenclature, in the following, 'resilience analysis' will be used as a broad term, in line with risk analysis, to include resilience assessment, resilience characterization, resilience communication, resilience management and policy relating to resilience. As discussed in Section 3.1, risk analysis covers applied risk analysis and generic risk analysis:

- Applied risk analysis A: Risk analysis of a specific activity (interpreted in a broad sense, also covering natural phenomena) in the real world
- Generic risk analysis B: Development of concepts, theories, frameworks, approaches, principles, methods and models to understand, assess, characterize, communicate and (in a broad sense) manage risk.

Similarly, applied and generic resilience analysis can be defined, by replacing the word 'risk' with 'resilience' in the above definitions.

When studying the nexus between risk and resilience, and risk analysis and resilience analysis, the generic part is of special interest, as it covers the basic ideas, concepts and principles of the field and science, guiding the applied analysis.

When studying the literature on the links between risk and resilience, it is possible to identify different types of perspectives. Three dominating categories seem to prevail, as shown in Figure 7.2. We refer to these as 'Risk analysis = Probabilistic Risk Assessment (PRA)', 'Different schools' and 'Unified approaches'. The 'Risk analysis = PRA' perspective goes back to the 1980s, when the risk field was strongly built on risk assessment and a rather technical probabilistic understanding of risk. See discussions in, for example, Park et al. (2013) and Linkov et al. (2016). Following this perspective, there is a quite small overlap between the risk and resilience fields. As mentioned in Section 1.5, the resilience analysis field was developed as a supplement to PRAs, acknowledging that important aspects of risk and safety are not adequately captured by the traditional risk assessment methods (e.g. Hollnagel et al. 2006).

The 'Risk analysis = PRA' perspective remains common, particularly in engineering environments, where quantitative risk analysis is extensively used to guide the decision-making related to risk (see e.g. Aven and Vinnem 2007). Here, resilience analysis is not really acknowledged as a strategy for handling risk. This is illustrated by the common use of pre-defined quantitative risk acceptance criteria, prescribing what the proper risk level is, and

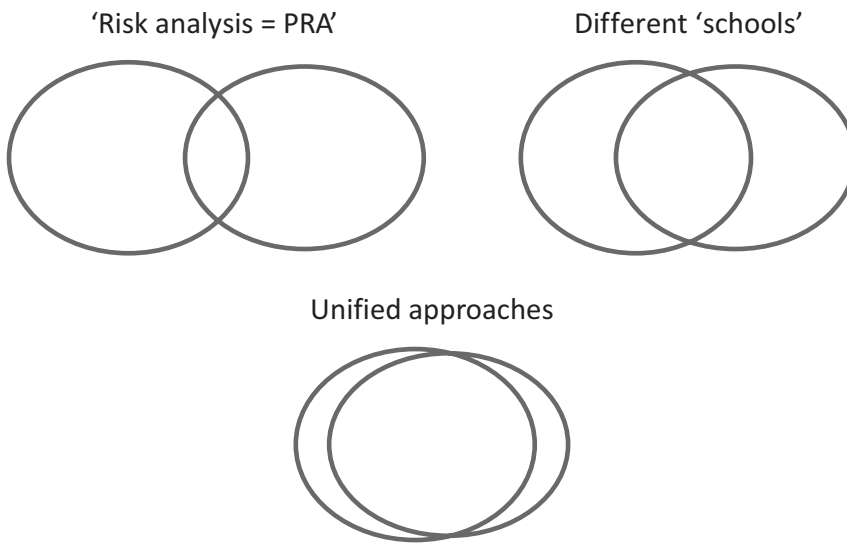


FIGURE 7.2 Schematic illustration of different perspectives on the link between risk and resilience analysis. Circles to the left represent the risk analysis field, circles on the right, resilience analysis

the related risk management process, in which risk assessment supports the risk treatment (see e.g. ISO 2018). Resilience analysis has no visible place in this process.

However, more balanced perspectives exist, also in engineering environments, in which the 'risk analysis school' acknowledges the importance of resilience and vice versa. Yet, we see a trend of separation between the schools, one centred around risk, the other around resilience. As noted in Section 1.5, much of the resilience research completely ignores risk considerations, and vice versa.

The third category of perspectives is different. Here, some unified risk-resilience approaches are sought. Risk and risk analysis are broadly defined, and resilience and resilience analysis constitute basic pillars of the risk field and science (Renn 2008, Aven 2017a). For many of the issues society faces today, characterized by large consequences and uncertainties, resilience analysis is considered a backbone of risk analysis. The present book is based on the 'Unified approaches'.

Following the risk conceptualization made in Sections 4.2 and 7.3, we can write:

$$\begin{aligned}\text{Risk} &= (A,C,U) = (A,U) + (C,U|A)\\ &= \text{“occurrence of events, and associated uncertainties”} +\\ &\quad \text{“consequences given events, and associated uncertainties”}.\end{aligned}$$

In line with, for example, SRA (2015a), resilience can be defined as the ability of the studied system to maintain functionality and recover, given that one or more events A occurs, whether these events are known or not. Hence, resilience is strongly linked to (C,U|A) in the above formula. If, for example, C equals the number of fatalities in relation to the operation of a process plant, (C,U|A) expresses this number and associated uncertainties, given that the event A has occurred, for example a fire. The system's ability – and lack of ability – to continue functioning and recover will determine C.

As another example, let C denote the time the system state is below a desired level L. Given the occurrence of an event A, which causes the system to 'jump' to a failure state below L, the consequence C then expresses the time it takes to recover, i.e. be in a desired state L or better (we simplify and assume that in the interval considered, the system is in a state below L maximum one time, and the system state is L or better at the end of the interval). Then risk can be seen as (C,U), the risk of failure and downtime time in the period considered, and resilience as (C,U|A), the recovery time, given the occurrence of the event A, and associated uncertainties.

We see that (C,U|A) captures important aspects of the resilience concept. We may by definition refer to (C,U|A) as resilience; alternatively, it can be phrased as the 'resilience-induced conditional risk' or 'lack of resilience-induced conditional risk' given the occurrence of A (Aven and Thekdi 2018). Alternatively, we could refer to (C,U|A) as vulnerability, as in Sections 4.2 and 7.3. Some authors prefer to restrict the vulnerability concept to situations where the event is A known, for example by expressing the probability of dying given a specific disease. In the above set-up, both known and unknown types of events A are allowed.

Following the above reasoning, we see that resilience is included in the risk concept and, hence, resilience analysis can be seen as a part of risk analysis. Think about a person who is subject to risk due to potential diseases. Here, A is the occurrence of a disease and C the effects on his or her health. The vulnerability or 'lack of resilience-induced conditional risk' (C,U|A) relates to the health condition of the person, given the disease. We may limit the effects to the event that the person dies (as is often the case for risk studies), but we could also include other effect states, including the return to a normal state, which is a typical focus of a resilience analysis. The framework is general and allows for and encourages the use of different types of specifications for C.

From the above set-up, a distinction is made between the concept of risk and how it is described or measured; see Chapter 4. In its broadest sense, risk is characterized by (C', Q, K), where C' are some specified consequences (for example, the number of injuries or fatalities, or the downtime of a system), Q is a description or measure of uncertainty (for example, probability and

associated strength of knowledge (SoK) judgements supporting the probabilities) and K is the knowledge supporting Q. Applied to the 'resilience-induced conditional risk' (C,U|A), we can analogously characterize it by (C', Q, K |A); refer to Section 4.2.

This type of conceptualization and characterization of risk allows for and stimulates unifying perspectives on risk and resilience and is used, for example, in Aven and Renn (2018).

Returning to the 'Risk = PRA' perspective, we quickly see what makes the interaction between resilience and risk difficult. As risk here is basically expressed through probability or expected values, often on the basis of historical data, there is little place for resilience analysis, as this analysis is to a large extent justified by referring to knowledge considerations: the knowledge supporting the probabilistic assessments could be more or less strong and there is a potential for surprises relative to the available knowledge. The probabilities do not reflect all relevant uncertainties. Using P as a generic symbol for probability, we can for this perspective schematically write:

$$\begin{aligned}\text{Risk} &= (A,C,P) = (A,P) + (C,P|A)\\ &= \text{“occurrence of events, and associated probabilities”}\\ &\quad + \text{“effects and related probabilities, given A”}.\end{aligned}$$

These representations are, however, not very useful in relation to events A which are not known. Probabilities in such situations provide little information.

For the 'Different schools' perspectives, there are no specific conceptualizations to refer to, as the basic idea characterizing the stand is that there is some type of indifference concerning what the other school is actually thinking. The resilience school is concerned with developing its own concepts and methods; it is not trying to integrate risk and resilience perspectives. The same is the case for the risk analysis school.

7.4.2 Discussion – the call for a shift from risk to resilience

Consider medical research. To a large extent, it concerns identifying potential diseases – and their 'causes' – and how to best treat them. It captures the essence of risk analysis. No one would seriously question the importance and need for this type of research and analysis. Think about the penicillin antibiotics, which have been so effective against many bacterial infections. Risk analysis is clearly justified. There are many drivers for medical research, including considerations of where the potential to have the greatest impact is the strongest: in other words, where risk can be most effectively reduced or managed. Risk considerations are, thus, also needed for this purpose,

although probabilities could be difficult to determine as the knowledge base could be rather weak.

Resilience analysis alone is not enough. It would be a poor policy to think only about strengthening the resilience of the human body to meet potential diseases. But it would also be a poor policy not to acknowledge the importance of and need for resilience analysis. With a strongly resilient system, the disease risk could be strongly reduced. The message is thus clear. We need both risk- and resilience-based considerations and measures.

The probabilistic perspective is too narrow

In view of this, the call for a shift from risk to resilience must be interpreted as a call for stronger weight to be placed on resilience and resilience analysis. This means that narrow probabilistic-based risk perspectives should not in general be used as a basis for risk decision-making. As discussed in Section 7.3, these perspectives do not give resilience the place it deserves. Traditional risk frames are not suitable for guiding the decision-making on choice of arrangements and measures. In the face of uncertainties and the potential for surprises, we need to develop resilient systems. For example, extreme weather events of different types – also surprising ones – occur, and we need to build systems that are able to meet these. As discussed above, this cannot be done without some type of risk consideration and risk handling – resilience and risk analysis are both needed.

The need to fight back against the 'Different schools' perspective

Changes are therefore required when it comes to the 'Different schools' perspectives. Separation is not the way forward. Institutions stimulating integration need to be encouraged and supported. This also means bridging the gap between different scientific environments and communities, in particular between more technically oriented scholars and social scientists. Risk assessment is mainly technical, whereas social scientists dominate the resilience field. However, as argued for above, the problems to be solved require both risk and resilience-based thinking. Seeing these two areas as distinct fields and sciences is thus problematic. The differences will grow bigger and probably also lead to less innovative approaches and methods. We should therefore fight back against the 'Different schools' perspectives.

'Unified approaches'

There could be different platforms for improving the understanding of integrated risk-resilience perspectives, but they will all be built on an acknowledgment of the importance of the other field, to adequately

understand and handle risk and resilience. The 'Unified approaches' make such acknowledgements and use integrated risk and resilience concepts to build holistic and comprehensive methods and models for meeting real-life issues. The above argumentation has shown that risk analysis is a more overriding perspective than that of resilience, but the key is to acknowledge the importance of both risk and resilience. The crucial role of resilience in improving systems and handling risk makes it essential that resilience analysis is also developed.

As an example of the benefit of integrative perspectives ('Unified approaches'), think about the way resilience is typically analysed using probabilities and expected values, given a specific event A. As discussed in Section 7.4.1, risk research provides argumentation and guidance on how to extend such methods based on (C',P|A), by considering the broader conditional risk concept and characterizations (C,U|A) and (C',Q,K|A). Consider, for instance, the time T it will take for the system to regain normal functioning given a disturbance. Typically, a probability distribution or the expected value of T would be used as metrics in this case. Introducing the (C,U|A) and (C',Q,K|A) perspectives would, however, add considerations that extend beyond these metrics to reflect the strength of the knowledge supporting these metrics, as well as the potential for surprises.

The 'Unified approaches' stimulate integrated research on issues related to risk and resilience, which is basically absent in the 'Different schools' perspectives. In the latter case, research is conducted based on some founding ideas, as formulated by Hollnagel and other leading scholars in the field. A key element in this research is a focus on system functioning and success rather than failures. These perspectives have led to new insights, as well as methods for analysing resilience. The 'Unified approaches' supplement this type of research by incorporating risk conceptualizations and principles. This enriches the pure resilience-based research, as risk is fundamentally linked to resilience, as discussed above, but this is seldom reflected in the resilience research. Similarly, the 'Unified approaches' would stimulate the incorporation of resilience type of knowledge into the risk research. Signals and potential surprises are rooted in resilience thinking but not so much in risk science.

Conceptually, the above analysis shows that resilience can be included in the risk concept, as resilience is broadly speaking about conditional risk, and, hence, resilience analysis can be seen as a part of risk analysis. However, in practice, we need to highlight both resilience and risk. When studying resilience, we also need to consider risk, and, as such, it is possible to argue that risk analysis is also contained in resilience analysis. Depending upon the research question or focus, resilience analysis could be a means towards risk analysis and vice versa.

The improvement aspect and the concept of 'antifragility'

Traditionally, the resilience field has focused on regaining the performance of the system, but, recently, the improvement aspects have also been highlighted. However, the term 'resilience' as such does not really point to improvement in system performance as a fundamental feature. Rather, it is a recognition of the need for thinking along these lines that has led resilience scholars to extend the scope of the resilience field. Similarly, it can be argued that the risk field has devoted little attention to learning and improvements. The concept of antifragility by Taleb (2012), see also Section 3.2, is an example of a contribution which meets this gap in both camps. The idea is that some types of stress, risk and uncertainties need to be welcomed – 'loved' – in order for the system to become better over time. It is not enough that the system is robust or resilient. The concept can be seen as a development within the "Unified approaches" (Aven 2015a).

Risk and resilience assessment methods

Risk assessment is commonly used in practice. Although the scientific quality can be questioned in many cases, the risk assessment tool works. One of the reasons for this is that simple, practical methods exist for how to conduct the assessments. The resilience field has pointed to limitations in many of the current risk assessment methods, particularly in relation to complex systems. However, alternative approaches and methods have, to a limited degree, been developed. Although methods like FRAM and STAMP (Hollnagel et al. 2006) are often referred to, they are not really risk assessment methods but, rather, approaches for understanding the system performance (Bjerga et al. 2016). In all types of analysis, a balance must be struck between accuracy and simplicity, and, for many types of risk issues, simple models and methods, as traditionally used in risk assessment, work fine and can be justified. However, for other cases, typically characterized by large uncertainties, these models and methods are not suitable. The 'Unified approaches' seek the development of holistic models and methods, which reflect both risk and resilience. The 'Different schools' perspectives have little to offer, as such models and methods cannot be founded on 'narrow perspectives' on either risk or resilience. More research is needed to develop practical models and methods that can analyse resilience in a risk framework; refer to the discussion in Bjerga et al. (2016).

The development of a distinct resilience science

There is a growing acknowledgement that risk analysis can be seen as a distinct science, comprising applied and generic risk analysis (SRA 2017a, b),

as defined in Sections 3.1 and 7.4.1. Resilience analysis is developing as a field and science, but the same type of acknowledgement is not yet observed. However, to further develop resilience analysis, a scientific foundation is required, and the framework presented in Section 7.4.1 provides such a foundation, consistent with the risk field and science. An acknowledgement of resilience analysis as a science, with a generic and an applied part, would trigger a need for clarifications of what this science is, compared to risk analysis as well as to other fields and disciplines. The call for a shift from risk to resilience underlines the need for resilience analysis to be further developed. Recent reviews of resilience analysis point to many challenges (Patriarca et al. 2018), including how to measure, describe and characterize resilience (Haimes 2009, Hosseini et al. 2016, Aven 2017d); how to link resilience and risk (Bergström et al. 2015, Aven 2017d, Zio 2016, 2018); and how to best develop and design resilient systems (Bhamra et al. 2011, Dinh et al. 2012). Different types of approaches and methods are used; see, for example, the review by Curt and Tacnet (2018), which shows that network/graph theory-based modelling is popular in this research. Much fundamental research linking resilience and risk has not been identified. As argued for in Section 7.4.1, it is possible to take the perspective that resilience analysis is an integrated element of the field and science of risk analysis. The call for a shift from risk to resilience highlights the need for the resilience element to be strengthened.

7.4.3 Conclusions

Resilience analysis has developed as a reaction to narrow risk analysis. It has a rationale, as resilience is a main system feature influencing safety and risk. Two trends are now observed. The first is a growing separation between risk analysis and resilience analysis (the 'Different schools' perspective): here the other community is to a large extent ignored. It is a development that is counterproductive. Neither risk nor resilience can be properly analysed and managed without thinking about both risk and resilience. The second trend ('Unified approaches') acknowledges this need and seeks to develop holistic approaches integrating risk- and resilience-based thinking. The present analysis argues that this type of perspective is the one to further pursue. Only in this way can the call for a shift from risk to resilience be meaningfully interpreted. Resilience analysis needs to be further highlighted, but a risk analysis framework is required to ensure that the right questions, concerning threats, hazards and opportunities, are asked and the resources are used in the best possible way. Risk analysis and resilience analysis should join forces to improve the research basis and increase impact. It is urgent that the separation trend is stopped.

7.5 IMPROVING GOVERNMENTAL POLICIES: SOME FUNDAMENTAL PRINCIPLES

This section discusses the basic principles that a government should adopt when it comes to risk. There seems to be broad agreement about general principles, such as openness and transparency, involvement, proportionality and consistency, and making decisions based on evidence, but when it comes to a more detailed level, suitable principles are missing or are inconsistent. For example, what does it mean to base decisions on evidence or to act with proportionality when regulating or managing risk? The present analysis aims at stimulating a discussion on this topic by formulating eight specific principles that governments should apply for the effective treatment of risk in society, based on recommendations by Aven and Renn (2018). Several examples are used to illustrate the discussion. Much of the discussion is also relevant for organizations and companies, but there are differences; see, for example, Aven and Thekdi (2019) for a discussion of principles relevant for enterprise risk management (ERM).

7.5.1 What is really the issue?

All activities are subject to risk; each of them will result in one and only one outcome, but which one we do not know today, since there are uncertainties. Hence, anticipating this outcome is a challenge. There are uncertainties about future developments, relationships between causes and effects, and context conditions (Renn and Klinke 2016). Examples of such uncertainties include the performance of nuclear repositories for thousands of years, the regional distribution of climate impacts due to the increase in greenhouse gases, the spread of infectious diseases, and the type, magnitude and number of terrorist attacks. Looking, for example, at the coming year, a pandemic may or may not develop, yet we need to make decisions regarding whether it is prudent to allocate resources to prepare society for such an event. The tool for informing this decision is risk analysis. Experts assess the risk, using the knowledge they have on the topic. They make predictions of what will or might happen, but they face uncertainties. How reliable or trustworthy are these risk assessments? How much confidence can risk managers and regulators place on these assessments when they have to make decisions on how to treat these risks before they possibly materialize?

Swine flu case

A good case in this respect is swine flu in 2003 and 2009. The WHO (World Health Organization) declared that the flu had developed into a world epidemic, and a vaccine was hastily developed (WHO 2009). There were

reasons to believe that the flu would cause serious illness and problems. To limit the epidemic, it was important to act quickly, and some governments implemented extensive public relations campaigns to get people vaccinated, despite the fact that the vaccine had not been thoroughly tested for side effects (Munsterhjelm-Ahumada 2012). Governments were faced with a dilemma. They had to balance the need for action, to meet the risks linked to the spread of the epidemic, and the risks related to potential side effects. Quick and extensive vaccination might control the disease and reduce damage, but it would also impose some level of risk on the population, as there could be severe side effects from the vaccine. The degree to which the risks were faithfully characterized, also addressing possible unknown side effects, is open to discussion (Dowdle 2006, Aven 2015b). In public communication, most governments opted to advertise or even subsidize the vaccination without mentioning the potential side effects. The side effects were not an issue in the governmental communication efforts, at least in the Nordic countries (Aven 2015b). The general criterion of being open, transparent and balanced about the understanding of the nature of risks to the public suffered. The decision was difficult for the authorities because of the time pressure; they had to balance judgements concerning the development of the flu, the efficiency of the vaccination, risk and uncertainty issues, as well as ethical aspects (Aven 2015b).

From a risk management and risk governance perspective, the case illustrates that dealing with uncertainties and different values in risk management is not a trivial task. It involves serious reflection on trade-offs and conceptual thinking about the nature of proper policy guidance (Frewer et al. 2002). The swine flu case relates to many key principles and features of risk management and governance, including:

- The characterization of risk in the face of large uncertainties
- The need for proportionality and consistency in decision-making
- The choice between various management approaches, such as the cautionary and precautionary principles, and the risk-assessment approach
- The role of risk perception in risk management
- The best way of communicating risk
- The trade-off between openness and transparency versus effectiveness and efficiency

Different countries have developed different strategies and policies with respect to the issues mentioned above. There are always dilemmas, calling for a balance to be made and also compromises, as the swine flu case illustrates. Governments would like to know in advance the likely impacts of each of their decision options based on the best available knowledge, but what does this mean in practice when we face risk and uncertainties?

An interesting concrete example showing the core elements of a governmental risk management policy is the UK document published by the House of Lords (UK 2006). It states that, in brief, the guiding principles of governmental risk management are:

- Openness and transparency—Government will be open and transparent about its understanding of the nature of risks to the public and about the process it is following in handling them
- involvement—Government will seek wide involvement of those concerned in the decision process
- proportionality and consistency—Government will act proportionately and consistently in dealing with risks to the public
- evidence—Government will seek to base decisions on all relevant evidence
- responsibility—Government will seek to allocate responsibility for managing risks to those best placed to control them.

(UK 2006)

The swine flu example shows that, in practical situations, these principles are not easily implemented. Moreover, the principles are all noble, but they may contradict each other in many cases or lead to ambiguities in terms of what is at stake and what is the most suitable decision option. It is common to distinguish between three major strategies for managing or governing risk: risk-informed, cautionary/precautionary and discursive strategies, as discussed in Sections 3.1 and 7.1. However, relatively little scientific work has been devoted to the challenge of formulating and discussing how these various principles and strategies interact and how they can be made operational for governments when dealing with risk. The present analysis addresses this challenge, by integrating general governmental criteria, as illustrated by the UK (2006) policy document (see also e.g. MI & E 2014 and OECD 2017), as well as scientific literature providing arguments for how to manage and govern risk.

7.5.2 Eight key principles guiding governments on how to deal with risk

In the following, we will present and discuss eight principles guiding governments on how to handle risk, based on work by Aven and Renn (2018):

1. In general, the proper risk level is a result of a value and evidence/knowledge-informed process, balancing different concerns. To develop values, risk taking is needed. How much risk to accept in pursuit of value is dependent on both context and how values are weighted.

2. This process of balancing different concerns can be supported by cost-benefit balancing methods, but this type of formal analyses needs to be supplemented with broader judgements of risk and uncertainties, as well as stakeholder involvement processes.
3. To protect values like human lives and health, and the environment, the associated risk must be judged to be sufficiently low.
4. Risk perceptions need to be incorporated into risk governance but with great care.
5. Three major strategies are needed for managing or governing risk: risk-informed, cautionary/precautionary and discursive strategies. The cautionary/precautionary strategy is also referred to as a strategy of robustness and resilience. In most cases, the appropriate strategy would be a mixture of these three strategies.
6. Governments should be open and transparent about their understanding of the nature of risks to the public and about the process they are following in handling them.
7. Governments should seek to allocate responsibility for managing risks to those best placed to control them.
8. Intervention is needed in the case of market failure or equity issues.

There is no ranking in the order of appearance of these principles; however, some of the most fundamental propositions come first.

1 In general the proper risk level is the result of a process balancing different concerns

In general, the proper risk level is the result of a process balancing different concerns (value generation, cost, safety, personal freedoms and civil liberties, etc.). Activities in life, industry and society are initiated and performed to obtain something of value; refer to Section 7.1. This is normally called benefit. Benefit describes an outcome that people value positively; this could be material or non-material goods. We build nuclear power stations for the purpose of developing energy, we invest in infrastructure to improve the transportation of people and goods, we send people to the moon to explore space, etc. However, there are always some costs – interpreted in a wide sense – associated with the activities. These costs also include risks related to the potential negative side effects of these activities. The risk is not the main driver for the realization of the activities. Rather, risk is something, related to the activity, that we need to take into account when making decisions on whether to initiate the activity or on how to best perform the activity if realized. It must be acknowledged that generating benefits and value requires a certain degree of risk taking. Therefore, we need to compare the benefits of the activity with the costs and these risks, and then

make a decision on whether the benefits outweigh the costs and risks, or the costs and risks outweigh the benefits.

In a second step, we also need to decide how we can reduce the costs and risks without compromising the benefits. In the balance between benefits, costs and risks, risks are rarely taken for their own sake (only risk as a thrill); the risks are accepted or tolerated because a *positively valued service to individuals or society as a whole* is sought that provides more good than the bad linked to the associated risk (Fischhoff et al. 1981, Smith 1986).

However, the juxtaposition of benefits versus costs and risks is not straightforward. There are two major issues:

a) The first relates to the value diversity in a plural society. The judgement about what people value as a benefit or a disbenefit may differ from group to group and from individual to individual (Shrader-Frechette 1984). For example, an activity that promises to promote industrial growth will be welcomed by most economic stakeholders but may be regarded as a disbenefit by many environmental stakeholders, fearing additional environmental degradation. Furthermore, goods are not equally distributed. A financial gain by a transaction that benefits the 1 per cent richest people in a society may be seen as a disbenefit by the poor (violation of equity principles), even if the poor are not worse off than before the proposed transaction (Pareto optimal solution). The question arises: who decides what outcome of an activity or decision option is framed as a benefit or a disbenefit or something in between? Often public risk managers and regulators focus on disbenefits, where almost all members of a society agree prima facie that this impact is not desirable, such as an increase in mortality, morbidity or environmental degradation. It is not by chance that most risk management agencies deal with these publicly affirmed disbenefits, as almost all members of society agree that the government has the duty to protect people from physical harm. Yet, even in those cases, differences in distribution (who will suffer the most and who will gain the most?) may impede collective decision-making rules when making trade-offs between benefits and disbenefits.
b) The second issue relates to the unavoidable uncertainties that are associated with the benefits and costs. Usually, the benefits are more certain than the costs (because the activity is meant to produce these benefits). Unintended side effects of the activity, for example the production of a specific good, may occur, as there are risks. Some of these risks may be anticipated, others not (Baram 1980). Loosely speaking, the less experts know about an activity or intervention and the more this activity is shaped by changing context conditions, the more likely it is that society will experience some unpleasant surprises.

In a democratic and liberal market society, a basic thesis is that the value judgement of whether the costs-risks outweigh the benefits (or vice versa) should be left to the individual decision-maker, as long as this person is fully informed about the costs-risks and benefits (or at least has access to all this information), is mentally capable of making this judgement and, most importantly, the costs-risks and benefits can be limited to this individual (no major external effects). However, in practice, there are nearly always some external effects (Edwards and von Winterfeldt 1987). In addition, what does it really mean to be fully informed about costs-risks and benefits?

Think about the costs associated with smoking. An individual decides whether or not he/she would like to smoke, but the societal costs are huge and may justify measures to stop individuals from smoking. The result is that governments intervene and regulate. In the swine flu example, each individual had to make a choice – vaccination or not – despite poor knowledge about the risks related to this activity.

In addition to individual risk taking, society is confronted with collective risk taking, for example when national security is at stake. Other activities are on the borderline between collective and individual risks, such as ensuring food safety or licensing chemicals. People trust that the government is able to control these risks, such as food poisoning, or protect individuals if ignorance or misperceptions would lead to fatal or chronic results, thus providing little opportunities for individual learning (Pidgeon 1997). The boundary between individual responsibility for one's own actions and government's paternalistic regulation is fuzzy and depends on political convictions (right-left), political culture (libertarian versus individualistic) and historical traditions (tobacco versus soft drugs). Although it is a primary government task to protect the safety and health of its citizens, there is always a balance to be made, as the above examples illustrate. Most risk decisions touch upon more than just one dimension (for example, health, environmental damage, costs, etc.). Making rational judgements on different options hence requires the assignment of trade-offs. Trade-offs represent manifestations of value priorities that cannot be deducted from factual information alone but require political value judgements. In a democratic society, these value judgements need to be legitimized; paternalism would not suffice.

Oil and gas example

A case study about the oil industry provides a good illustration of this discussion (Aven and Renn 2012). The oil and gas industry in Norway has created huge value for Norway, but considerable risks have been taken, with respect to both investments and safety. A key principle of the governmental policy was that the state pays a main share of the investments and costs but also receives a corresponding share of the income from the production.

The state was thus willing to take substantial risk in exchange for the expected benefits. It was aware that the activity also implied substantial safety risks. Many accidents have occurred over the years and about 300 persons have lost their lives. In 1981, 123 persons were killed in the capsizing of the Alexander Kielland platform and there have been several helicopter crashes, the latest in 2016 when 13 people were killed. The benefits of the oil and gas production were considered to have such a huge potential that the activity was worth realizing, despite the risks. Given the huge benefits that have actually been created for the state over the last 50 years, there are few people today that would criticize the state for taking this risk. This may be quite different from other oil-producing states such as Nigeria or Venezuela.

Today, the situation is more complex, and Norwegian society is more diversified in its value structure and concerns. The country faces a fierce debate about the development of oil and gas fields in environmentally vulnerable areas (such as the Lofoten area). For many political parties and persons, there is much less willingness to take risks in exchange for the economic benefits than 20 years ago. Many believe that more oil development would mean doing a disservice to Norwegian society. The value of potential environmental damage has a stronger impact on the judgement than the value of greater economic prosperity. The issue is also related to the overall goals of reducing CO2 emissions. Some parties see an extension of the petroleum activities as being in conflict with these goals. It may also be true that it is easier to renounce the additional incomes induced by more oil exploration now, when the economy of the country is already strong.

Governmental policies need to find the proper balance between stimulating benefit generation and risk reduction. Some political parties and persons are more willing than others to take higher risks in pursuit of certain benefits. There is, however, no value-free balancing process that is acceptable to all stakeholders. There is no objective correct governmental policy. Different approaches and methods exist for supporting these balancing processes, reflecting different stakeholder values and available evidence/knowledge.

This Principle 1 means that, when making their decisions, governments seek to be informed by all relevant evidence from all relevant stakeholders. Evidence here includes relevant data and information, for example accident data and statistics, as well as knowledge in terms of justified beliefs derived, for instance, through risk assessments. The justified beliefs can be derived on the basis of observations, reasoning, modelling, dialogue, etc.

The above discussion has made it clear that the decision-making cannot be purely evidence-based (Mearns 2015, Löfstedt and Bouder 2017). Evidence may cover subjective judgements and beliefs from various stakeholders; these can be more or less strong and also erroneous in some cases. The beliefs can be based on assumptions that may turn out to be wrong.

Hence, decision-makers also need to address these limitations and uncertainties related to the knowledge basis. In addition, there could be different values related to the various concerns, as illustrated in the above oil and gas example, which could strongly influence the decision-making.

2 Cost-benefit type of analyses and the need for seeing beyond them to properly support the decision-making

Faced with many attributes and concerns, the decision-makers would ideally like to have a method that could guide them on which alternative or measure to choose, to ensure that the resources are used in the best possible way. The literature is full of theories and approaches that seek to meet this challenge by optimizing the decision-making according to such a goal. The most well-known scheme is the subjective expected utility theory, which has a strong rationale and appeal (Fischhoff et al. 1982, Lindley 1985). However, this approach is purely subjective and does not provide any guidance for the collective decision-makers on how to use their resources in an optimal way. The approach is also difficult to use in practice, with its demanding ways of specifying probabilities and utilities (Aven 2012a).

Cost-benefit type of analyses are more commonly used, particularly for governmental decision-making (Smith 1986, UK 2006, Jones-Lee and Aven 2009), and are thoroughly discussed in Section 7.2. They are attractive, as they aim to show how to best use the resources in relation to the options at hand. The analyses are well-established, standardized to a large extent and ensure traceability of the arguments used. All costs and benefits are transformed to one common unit, normally money, introducing concepts like the value of a statistical life (VSL). This value represents the amount of money the society is willing to pay to reduce the expected number of fatalities by one unit. In practice, the criterion used for comparing options and measures is based on expected net present values, E[NPV]. Hence, the contribution to the expected value from an accident leading to 100 fatalities having a probability p is taken as $100 \cdot \text{VSL} \cdot p$. The VSL concept is controversial, as thoroughly discussed in the literature; see, for example, Ale et al. (2015, 2018) and Aven (2012d, pp. 120–1). Using a concept like VSL does not mean that one specifies the value of a life. In principle, a life has an infinite value; there is no amount of money that a person would find sufficient to compensate for the loss of a daughter or son. However, a statistical life has a finite value, as societal decisions need to be made that balance different concerns – benefits, costs and risks. Otherwise, it would be impossible to assign any trade-offs. The VSL is a decision-support tool for this purpose. Thus, for groups of people, the use of VSL numbers can be interpreted as providing indirect specifications of the value of these lives.

As discussed in Section 7.2, the CBAs provide decision support and inform the decision-makers, but it must be acknowledged that they do not give much weight to risk and uncertainties. They represent, in fact, a tool that favours development more than protection. The use of such analyses consequently must be supplemented with specific assessments and judgements of risks and uncertainties; see also discussion by Ale et al. (2015, 2018). Hence, the common idea of using a fixed VSL number for different sectors and applications is also problematic and should not be implemented (as also argued by Ale et al. 2018). The approach ignores specific risk and uncertainties and could seriously misguide decision-makers. An example illustrating this discussion is the use of the ALARP principle; see Section 7.2 and Ale et al. (2015).

In addition to the need to reflect uncertainties and risk beyond expected values, issue a) mentioned in the previous section, concerning value diversity in a plural society, imposes limitations for the use of cost-benefit type of analyses. More and more decisions in a complex and plural society include multiple and often contradicting values and a high level of uncertainty of the consequences of the activities. In these cases, traditional balancing of aggregate costs and benefits is neither sufficient nor politically acceptable. Plural values demand a risk governance process that starts with a major framing effort to identify the concerns, expectations and associations of major stakeholders in the debate, in order to gain an accurate picture of the benefits and disbenefits associated with the activity. Facing uncertainty and different values demands a more careful balancing approach that is not limited to comparing statistical expected values for benefits, costs and risks. It requires special consideration of uncertainty and a more cautious approach to ignorance and surprise.

It is often stated that governments should seek proportionality and consistency in decision-making (Sand 2000). These goals seem obvious and rational at a first glance: we should not use many more resources in one sector compared to others, to obtain the same level of performance. For example, it would violate these principles if costly measures were to be prioritized in one sector to reduce the risk there, even if the risk situation is much more serious in other sectors and the costs for risk-reduction are the same. Unfortunately, this principle is not easily implemented in practice. How can we compare different activities with respect to risk? There are no objective ways of characterizing risk. We may compute various risk metrics, but caution must be shown in giving these indices a stronger authority than can be justified. Comparing, for example, traffic risks with nuclear power is not really possible using any type of risk metrics, as the potential for a major disaster is present in one case but not in the other. Governments should be informed by risk assessments, but it is not possible to provide easy and

direct comparisons across different sectors and activities. The use of cost-benefit type of analyses is a tool to ensure proportionality and consistency in decision-making, but, as discussed above, this tool does not really address risk and uncertainties and can therefore not alone provide clear guidance on how to make adequate risk decisions. Hence, we recommend adherence to the goals of proportionality and consistency in decision-making by means of broad comparisons of risk characterizations and other relevant cost-benefit attributes, giving due weight to all aspects of risk, including uncertainties and strength of knowledge judgements.

3 To protect values like human lives and health, and the environment, the associated risk must be judged to be sufficiently low

Following the 2011 Fukushima nuclear disaster, Germany has decided to phase out their nuclear power plants by the end of 2022 (Ethik-Kommission 2011), refer to Section 7.3.1. There is concern about both potential nuclear accidents and nuclear waste. The risks are not considered low enough to be acceptable. This judgement of unacceptable risks can be viewed as independent from the benefits that are associated with the generation of nuclear power. Philosophers call these risks inviolate or categorical: they cannot be compensated for by benefits, regardless of how plentiful they may be (Josephson 2002). The risks alone are enough to ban the activity. As mentioned in Section 7.3.1, the German Ethics Commission, which paved the way for the governmental phase-out decision, was divided on this account. Roughly half of the commission stated that nuclear energy is not acceptable because of its catastrophic potential, independent of the probability of large accidents occurring and also independent of its economic benefit to society. The other half based their decision on recommending the phase-out on a cost-risk-benefit comparison of nuclear energy with other energy-producing technologies and concluded that, under the present circumstances, other means of electricity generation were feasible with almost the same benefit but less risk than nuclear power (Renn 2015).

How should governments then proceed to determine which risks should be regarded as inviolate and non-compensational? Should governments formulate explicit criteria for what are unacceptable or intolerable risk levels, to protect human lives and health and environmental values? The scientific literature on risk management often refers to such criteria, stating what should be considered as unacceptable or intolerable risk in society and for industrial activities; refer to Section 7.1. The benefit of using such criteria is that a clear rule can be communicated, and some consistency can be ensured across different activities. In the literature, reference is commonly made to maximum

limits for individual risks and limits defined by f-n curves expressing the frequency f of accidents having at least n fatalities (Meyer and Reniers 2013).

However, in general, such criteria in the form of strict limits for maximum risk are problematic. First, as discussed in relation to Principle 1, the appropriate risk level cannot be seen in isolation from other attributes and concerns, particularly the benefits of the activity. There are no universal numbers expressing what should be regarded as intolerable or unacceptable. If such criteria should be specified, they need to be determined so that they do not conflict with or hamper activities that provide a potential for major societal benefits. For this reason, many analysts suggest that such risk thresholds are defined for a set of activities that provide roughly the same benefit. For example, arguments can be provided for regulating indoor air pollution in factories, so that no more than 1 in 10,000 will get cancer as a result of exposure to a chemical in the air. This is independent of the production, as long as the goods produced are considered to have roughly the same benefit. Similarly, one could set a limit related to fatalities for any kilowatt hour produced, regardless of what the fuel for the generation of the electricity may be. Such limits act as clear statements of what risk levels the governments accept or tolerate in exchange for one unit of a desired service. Producers of the respective activity would then need to focus their work on demonstrating that the risk is acceptable or tolerable, by reference to the threshold or standard prescribed by the risk regulators. There may be additional requirements in the regulations to further reduce the risk, as for example in the oil and gas industry, where the ALARP principle is a legal requirement in many countries, but these are often difficult to implement as long as the absolute criteria exist, as discussed, for example, by Aven and Vinnem (2007) and Khorsandi et al. (2012).

If such maximum standards are defined and enacted, they need to be checked to see whether they are met or not. However, if, for example, probabilistic criteria are defined, as in the above examples, the measurement issue is critical. The risk numbers derived or estimated would normally be very much dependent on the analysts and their approaches, methods and assumptions. Uncertainty is a main problem here, too. Risk is not adequately described through numbers alone, like probabilities, as discussed in Section 4.2. Essentially, risk measurements or description capture three dimensions (consequences, judgements of uncertainties, and knowledge basis) and, in most cases, any attempt to reduce risk descriptions to one dimension will lead to poor assessments and judgements.

So, what are we then recommending governments to do?

To make decisions about permitting an activity or not, governments need to be flexible in balancing different concerns. Overall qualitative objectives that reflect the concerns of the major stakeholders may be formulated

to highlight areas that should be given special attention and priority, but strict criteria in the form of general thresholds for risk (un)acceptability across a variety of activities will reduce the necessary flexibility, will not give adequate justice to each situation, may cover or conceal important aspects of risk and uncertainties, and will experience major acceptance problems by those affected.

In particular, risks that are regarded as inviolate and non-compensational should not be linked to a specific numerical threshold, for example the maximum number of people killed in an accident. Such judgements also depend on the preferences and perceptions of those who make the risk decisions or are affected by them. In the aftermath of the Fukushima accident, Germany opted for phase-out, while the United Kingdom opted for nuclear energy expansion.

Broad risk assessments are needed to inform decision-makers. Risk assessment results should be evaluated with the purpose of informing decision-makers rather than concluding on a finite judgement about unacceptability, intolerability, etc. (Hale 2015). Typical risk numbers for similar activities to the one studied can be informative and used as a basis for comparisons, while acknowledging the need to see them in the proper context, taking into account uncertainties, strength of knowledge, supporting evidence and choice of assumptions, etc. Sometimes, if the environments are quite similar, it may help to have the same standards for all situations in order to demonstrate consistency and fairness. Yet, such an approach needs to be implemented with care; deliberation processes are needed, not automatic rules that are intended to fit all situations (Renn 2008).

4 Risk perceptions need to be incorporated into risk governance but with great care

Reference is made to the discussion in Section 6.1. The message is that public input on risk perception is important for (i) identifying concerns but not necessarily for measuring their potential impacts and (ii) for providing value judgement with respect to unavoidable trade-offs in the case of conflicting values or objectives.

5 Three major strategies are needed for managing or governing risk: risk-informed, cautionary/ precautionary and discursive strategies

Being risk-informed means both using risk assessment to understand and characterize risk, reflecting potential impacts – their sources and their effects, likelihood and related knowledge aspects (such as judgements of the strength of knowledge supporting the likelihood assessments) – and being

aware of and attentive to public perceptions and concerns. The risk and concern assessments inform the decision-makers, as highlighted many times already. The assessments are methodologically justified judgements made by the risk analysts and related experts in the field of study. The risk characterizations, which traditionally have been in the form of some type of probability statements, are conditional on the analysts' and experts' knowledge. In this sense, the risk characterizations can be viewed as conditional on experts' methods, data reliability, modelling assumptions, etc. The decision-makers would prefer unconditional assessments that can be taken as 'true, objective' values that they can use for costs-risks-benefit balancing. Instead, they are faced with a variety of assessments, sometimes contradicting each other. Furthermore, as explained above, these assessments may not cover all the concerns that people associate with the risk source and do not address the resolution of conflicting values and the trade-offs that are required. The results of risk assessments may all be informative in the sense that they give insights about some aspects of the risks, but there are still open issues, as the knowledge on which these assessments are built could cover or conceal risks. Thus, for the decision-makers, there is a need to see beyond the risk assessment, to properly take risks and uncertainties into account, as well as attributes and values not considered in the risk assessment (Edwards and von Winterfeldt 1987, Aven 2016a).

For many risk issues, the risk assessment results are not controversial, and the knowledge is sufficiently strong to produce a functional relationship between probability and amount of damage that is empirically proven and theoretically sound. In this case, a risk-informed strategy on the basis of formal risk assessment provides a clear rationale for risk reduction and also for risk communication (Aven and Renn 2010). Many routine risk situations fall into this category, such as wearing helmets when riding a bicycle, limiting the concentration of chemicals well below the threshold of toxicity, requiring passengers to wear seatbelts, setting building codes for the stability of constructions and fire prevention, or banning fluids from being brought onto an airplane. Most of these routine risk-based decisions are not controversial. They cover a wide range of daily activities, and scientific risk assessments have made a major contribution to the reduction of these conventional risk problems over recent decades (Renn 2016).

If we go beyond conventional, routine risk situations, the picture becomes more blurred. As previously discussed, many particularly complex risk situations require a broad set of multiple characteristics with trade-offs between them. Assigning trade-offs, in turn, depends on the underlying value priorities of those who perform the judgement. In a democratic society, these judgements need to be part of a due process legitimized by democratic institutions.

In addition, there are often considerable uncertainties related to the consequences of each decision option. For both reasons, uncertainty and value differences, a risk-informed approach is not sufficient and needs to be augmented with other principles, mainly the cautionary strategy in the case of high uncertainty and the discursive strategy in cases of different values (Klinke and Renn 2012, Aven and Renn 2010), see also Section 7.6.

Let us start with the case of high (or deep) uncertainty. We can choose swine flu as an example: here, we face major scientific uncertainties about the consequences of the swine flu. No reliable prediction model was available at the time. Risk assessment could have been performed but, because of the uncertainties, the assessments provided only poor knowledge about the consequences and the fraction of people that would be affected. Yet, the authorities needed to act to avoid serious damage. In most European nations, the authorities applied the precautionary principle, which invokes that, in the face of scientific uncertainties about the consequences of an activity, protective measures should be taken to reduce risks.

At first glance, it may seem intuitively plausible to act according to this principle. Yet, if doing nothing is also seen as a decision option, the principle may lead to dilemmas. This can be illustrated again with the swine flu example. What does the precautionary principle mean from the perspective of each individual who is confronted with the choice of getting vaccinated or not? Each person will be exposed to the side effects of the vaccination, again associated with uncertainties. The decision not to undertake vaccination can be interpreted as an application of the precautionary principle on the individual level. Many people did in fact select this option and avoided vaccination. From a scientific perspective, the odds of suffering from negative side effects caused by the vaccine were judged as significantly lower than the odds of contracting the disease. However, both judgements were associated with a high level of uncertainty, so that unanimous proof in the form of a clear-cut risk assessment was not available.

We are therefore left with a dilemma: the general rule of precaution can lead to different conclusions, depending on the choice of the default option and whose perspective we take (Renn 2009). If we regard vaccination as the default option, we should make sure that almost everyone is vaccinated, in order to be on the safe side when there is a danger that the flu might spread throughout a population. If, however, non-vaccination is the default option, we would opt for abstaining from any vaccination campaign, since there may be negative side effects associated with the vaccination. Both judgements can be justified with reference to the precautionary principle. The example demonstrates that the application of the precautionary principle cannot be seen in isolation from judgements of risk, uncertainties and other concerns. From an individual perspective, non-vaccination may be seen as

the natural default option, and then the application of the precautionary principle needs to be balanced against the risk related to contracting the disease. From the societal point of view, the natural option is the opposite, and the application of the precautionary principle has to be balanced against the risk of getting serious side effects.

Many risk theorists have addressed this problem and there are many suggestions for how to interpret the principle and deal with this dilemma (Charnley and Elliot 2000, Klinke and Renn 2001, Stirling 2007); refer also to the discussion in Section 7.3. In practice, the precautionary principle has been invoked when a new chemical or a new activity has been proposed and, given large uncertainties, the pure plausibility of such impacts was enough to justify regulatory actions. It seems wise to protect society from risks characterized by a weak knowledge basis, but it needs to be used with care as discussed in Section 7.3. The cautionary principle extends the precautionary principle. It is supported in robustness and resilience-based thinking and management (governance); refer to Sections 7.3 and 7.4.

The above dilemma identified for the precautionary principle will also occur in relation to the cautionary principle. In risk management and governance, there will always be a need to balance different principles and concerns. Yet, such principles can provide useful guidance, as they point to how to think and what aspects to consider and give weight to.

The third strategy is closely related to the experience of value differences in society. As risk judgements are multi-dimensional constructs, it is hard to imagine that any decision option will be dominant in all dimensions and meet all the values of the affected populations. Most collective decisions today face conflicting values and objectives. This is also true for risks. In addition, many individuals and groups may question the justification of or need for the foreseen benefits. Examples here are pesticides and therapeutic cloning. In cases of strong value differences and conflicts, a third approach to risk management and regulation is required: the so-called discursive strategy (Renn and Klinke 2016). This strategy is essential to reach societal consensus on the type of values and choice of objectives that the respective society will or should pursue when making collectively binding decisions, or on what priority should be given to what kind of values when trade-offs are being made.

Discursive methods of risk governance are not a one-way transmission of information from the authorities to the public, expressing the 'facts about risk', as was previously common, for example when authorities were arguing that an industry is safe because of some low calculated probabilities. Rather, the point of departure is the acknowledgement that risk cannot be captured by a single dimension (for example, expected cases of cancer per year) but requires a reflection about the potential benefits and risks (costs) from a

broad plural value perspective, including public concerns and risk perception. Dialogue and public involvement processes revealing the different positions and perspectives can, in many cases, lead to an improved understanding among relevant stakeholders, increase awareness of and sensitivity to the dilemmas and concerns that are at stake, and explore common ground for making the necessary trade-offs. If these processes are well designed and conducted, they may lead to a common understanding of the problem and widespread support for a risk management solution. A successful example is the three-party dialogue introduced in the Norwegian oil and gas industry, where a formal collaboration is established between the authorities, the industry and the unions (Bang and Thuestad 2014, Lindøe and Engen 2013, Rosness and Forseth 2014).

In summary (see also Section 7.6.2): for most of the routine cases of decision-making, formal methods such as risk analyses and cost-benefit analyses are adequate. They are effective in terms of public protection and efficient with respect to wise use of resources. However, tests should be performed to ascertain whether risk management decisions and/or regulations violate fairness principles or other forms of values, and whether the decision situation is associated with more uncertainty than appears at first glance. If the risk situation is characterized by high uncertainties, weight should be given to the cautionary strategy. Extra efforts at risk reduction and prevention could be justified. These extra efforts rarely include bans or prohibitions but, rather, limitations in distribution (space and time), in order to avoid irreversible decisions and strict monitoring and containment requirements. Finally, if risks invoke many conflicting values or concerns, a discursive strategy is required that provides a process of deliberations and stakeholder involvement, aiming at a societal consensus of compromise when assigning trade-offs.

6 Government should be open and transparent about its understanding of the nature of risks to the public and about the process it is following to handle them

See discussion in Sections 6.2.3 and 8.2.

7 Governments should seek to allocate responsibility for managing risks to those best placed to control them

This principle is based on the conviction that the risk management of any activity is best carried out by those who can control the activity. It reflects the basic idea that "One cannot be held responsible if one is not in control". Risk related to driving a car is best dealt with by the driver, whereas the swine flu risk needed national and even international handling, as the threat is intrinsically borderless. A fundamental principle often applied in industry is internal control, meaning that the company has full responsibility for the activities it

runs, including the risks (Delogu 2016). This principle has two aspects. First, it requires that inspection, monitoring and control are performed at the lowest possible governance level, while the rule-making should be arranged at the highest possible level, to ensure fair treatment of all constituencies and equal access to markets and innovations. The rules should apply to all (within limits), but implementation and control should be carried out at the local or regional level. Secondly, the rules should state the goals and objectives of the regulation; the various means of how to meet these goals should be left to the institutions that are obliged to manage the risks. For example, regulation may require that a company reaches a specific target emission; how this emission is accomplished, by changing production processes, installing more filters or substituting material, is for the company to decide.

As for all such principles, the targets must be implemented with flexibility. The risk management related to driving a car cannot be left to the driver alone. Society has introduced many measures and constraints to ensure that drivers can rely on safety features in their cars and on the assurance that other drivers are also qualified to drive a car. Drivers are hence obliged to obtain a driving licence, the car needs to meet specific technical quality requirements, speed limits are enforced, etc. Similarly, the internal control has many limitations, as society is not willing to allow companies to be totally flexible in how they meet standards and limitations. The choice of means may have other negative side effects, which makes it necessary to limit or regulate them, too. If pollution standards are met by using scrubbers and filters, which then need to be discarded in landfills, alternative options, such as changing the production process to avoid pollutants in the first place, may be required by state law. Furthermore, society rightfully involves agencies to check that the companies have implemented suitable systems that enable them to manage the risk properly.

In essence, governments should strive to allocate responsibility to those that can control the risks. There will always be limitations to this general principle, but those need to be justified. We consider it essential that as much as possible of the risk management is conducted by those that can best control the risks. Only then can we obtain the energy, innovation and creativity needed to maintain and improve the relevant activities and systems to avoid disasters. If the authorities are too specific about the means of risk management, it is obvious that efficiency will be sacrificed and often also the effectiveness in risk reduction.

8 Intervention is needed in the case of market failure or equity issues

There is much evidence showing that the use of seat belts is very effective in saving lives and reducing injuries in automobiles. For many years, however,

many car occupants did not use the belts, and the situation was considered a market failure (Arnould and Grabowski 1981). From a societal point of view, risk reduction could be substantially improved if a seat belt law were rigorously enforced. Governmental intervention was seen as legitimate, despite conflicting values like personal freedom. Smoking is another similar example.

There are many examples where equity issues have been neglected, in relation to both time (e.g. future generations) and social groups (e.g. exporting hazards to developing countries) (Kasperson et al. 1988). The way risk is commonly characterized, using losses and probabilities, and also the use of cost-benefit analyses, normally does not highlight such issues of distribution. Ethical considerations may, however, require regulatory action, even if the activity in total is cost-effective. For example, concentrating hazardous facilities in poor countries may be seen as a violation of equity, even if this provides revenues to these countries. Using national resources to build hospitals for the political elite, while the rest of the population is left with poor health care, is another example of equity considerations requiring regulatory intervention.

These are just some examples showing that interventions are justified in cases where desirable societal goals are not met, from either an economic or an ethical point of view. In practice, the issues are less obvious than in these two examples, but the two examples clearly show the need for correction. For further discussions of the ethical aspects related to risk and risk analysis, we refer to Hansson (2013b) and Ersdal and Aven (2008).

7.5.3 Discussion

The concern has been raised that our societies have become too risk-averse and that this development has a destructive impact on public policy and governmental risk management; see for example UK (2006). As suggested by the UK Prime Minister in a speech in May 2005, "We are in danger of having a disproportionate attitude to the risks we should expect to run as a normal part of life" and this is putting pressure on policy-makers "to act to eliminate risk in a way that is out of all proportion to the potential damage" (UK 2006).

It is not difficult to find examples where this type of concern is justified. The UK (2006) report mentions some examples, including defensive attitudes in the practice of medicine. Another example is the public management systems, commonly used today, which highlight bureaucratic requirements and reporting at all levels of the organizations. Over-regulation easily leads to a culture in which the main focus is compliance with these requirements

and criteria and not the overall performance of the organizations and their main functions, including the management of risk. The result is a lack of innovation and an impediment to changes that are required to advance the organization to meet the needs of the future.

Passive smoking example

However, at an overall level, there are reasons to conclude that governments in general manage and govern risk in a balanced way and that these concerns about too risk-averse policies are rarely justified. Let us use the case of passive smoking as an example. In recent years, we have seen a trend for governments to ban smoking in public places, often following intense discussion. The arguments for the ban relate to health and wellness, refer to Sections 3.2.2 and 7.3.2. In UK (2006), the evidence for such a ban is questioned. It is indicated that the decision to ban smoking in public places may represent a disproportionate response to a relatively minor health concern. This reasoning demonstrates the subjectivity of the framing of the problem raised by the bureaucrats that have produced this report. Their perspective is rather narrow and fails to incorporate several issues of importance for making the decision, for example the strong belief of people that they should not involuntarily be exposed to a risk source that is easy to avoid. Passive smoking is not only about lung cancer risks but also about the right of a person to use public places without being subjected to the health-damaging activities of others. Politicians need to take a comprehensive approach and reflect on all aspects, including changes in attitudes to smoking and passive smoking when such a ban is implemented. Experience from other countries has shown that people are pleased with the change, even if there was protest at the time of implementation. It is tempting to believe that many developments in society would not have been realized, if analysis alone had determined what ought to be the basis for making collective decisions, particularly when based on a one-dimensional risk assessment or traditional cost-benefit analysis. At the same time, risk assessment has been extremely helpful in reducing risks and making life in modern societies healthier and more comfortable over the years. As always, it is the delicate balance between regulation and freedom that makes the difference between investments into innovations and changes, on one hand, and preservation of the present condition, on the other.

Areas with a potential for improvement

If we look at the eight principles here recommended, most of these are at least partially implemented. Aven and Renn (2018) point to seven areas

where the potential for improvement is highest, when aiming for excellence in governmental risk handling:

a) The way to inform about risk. Informing people using probabilistic analysis is not sufficient. Broader characterizations are required; also, judgements of the strength of the knowledge supporting the probabilities are required, as well as considerations of potential surprises relative to the available knowledge.
b) The understanding that evidence is related not only to facts but also to beliefs and concerns that need to be incorporated into risk management and regulation, without going overboard by replacing assessments with public perception surveys.
c) The understanding that value judgements are equally important as a basis for decision-making as evidence in the form of data, information and justified beliefs.
d) The understanding that cost-benefit type of analysis can support but not determine decision-making. Balancing risks (costs) and benefits is crucial for making wise decisions, yet the net balance is often insufficient to address values other than mean risk reduction, particularly impacts on equity and distribution.
e) The understanding that, whatever tool is used to capture risks, it cannot provide a comprehensive answer regarding what is the best decision in relation to risk.
f) The understanding that risk-informed, cautionary and discursive strategies need to be employed, depending on the degree of uncertainty and value differences for the issue in question.
g) The understanding that the common rules for risk management and regulation should be made at the highest political governance level possible, but implementation and control should be organized at the lowest level reasonable.

To meet these challenges, risk assessment and management institutions, as well as regulatory agencies, should take greater responsibility for dealing with risk in a multi-objective, multi-value and multi-actor environment. Academic research and management expertise are both crucial for informing agencies and institutions on how to improve their performance and to strive for a better balance between necessary changes and cautionary approaches to protect what has been accomplished in the past.

Concerning the need for proper risk concepts and characterizations supporting the risk analysis as pointed to in item a, different frames can be used. One of the most general ones is presented by the SRA (2015a) Glossary and is adopted in this book.

7.5.4 Conclusions

Inspired by insights provided by the risk analysis field in recent years, eight principles that governments should apply in order to properly deal with risk in society have been highlighted. These eight principles can improve current policies and be useful for both bureaucrats and politicians, in their work in developing and implementing policies on risk management. They can be viewed as representing knowledge gained by the risk science. In relation to current practices, there is a potential for improvement that needs academic investigations and comprehensive expertise. These relate to both the understanding of the fundamentals of risk assessment, management and governance, and practical instruments to be used to conduct risk analyses and support decision-making. A main conclusion is that governments in general deal with risk in a fairly balanced way, but that they need to improve their understanding of the interface between facts and values in risk management. The use of cost-benefit analysis and concepts like 'evidence-based decision-making' are not obsolete, but they need to be enhanced with more risk- and dialogue-oriented policy styles.

7.6 SOME FOUNDATIONAL ISSUES RELATED TO RISK GOVERNANCE AND DIFFERENT TYPES OF RISKS

This section follows up the discussion on risk governance in Sections 1.6 and 3.2. In recent years, risk governance has become a commonly used concept in relation to the understanding, assessment, management and communication of risk or risk problems, including so-called systemic risks. Substantial scientific work has been conducted to establish a proper foundation for this concept and its applications. Nonetheless, there are still some issues that remain to be clarified, for example how to best characterize risks and risk problems that need risk governance approaches. The purpose of the present analysis is to provide new insights into the risk governance concept by critically examining common definitions and uses of key terms. In particular, the analysis seeks to shed new light on the interpretation of risk-problem classes: simple, complex, uncertain and ambiguous. A set of recommendations is presented on how to improve current risk governance theories and practices, including a suggestion for a modified risk-problem classification system.

If we think about risk analysis in the broad sense, as used in this book, it may be argued that there is no need for the concept of risk governance, as proper risk analysis should include all the features addressed by governance and risk governance. The analytic-deliberative process (Stern and Fineberg

1996, see also Section 1.6.3) is an example of principles adopted by risk analysis and so are other features highlighted by the risk-governance literature. We also see that there is an increasing acknowledgement of the need to think broadly when considering risk-management strategies – the three main categories of such strategies discussed in Sections 3.1.1 and 7.5 are increasingly recognized as the basic pillars of high-quality risk handling; see, for example, SRA (2015b). Common conceptualizations of risk also support this way of thinking, with their emphasis on uncertainty being a component of risk (SRA 2015a), see Chapter 4.

However, this change in perspectives on risk handling has been strongly influenced by the emergence of the field of risk governance. Substantial scientific work has been produced over the last 15 years on the topic, but equally important has been the practical guidance conducted by institutions such as the IRGC. The risk-governance school has developed from a need to broaden the risk thinking and approaches, as the prevailing mindset and methods were based on rather narrow conventional risk assessments using probabilistic analysis. Still, the common practice of risk analysis (in the broad sense of the term) is very much founded on probabilistic risk assessment, despite the fact that the type of problems considered extends beyond the 'simple'. The need for strategies also highlighting the cautionary/precautionary principles is still not broadly acknowledged. As a consequence, a strong focus on risk governance is considered essential for further developing the risk field. Through its emphasis on complexity, uncertainty and ambiguity, as well as systemic risks, the conventional narrow probabilistic perspectives on risk are challenged. It is to be hoped that with time the field and science of risk analysis (in the SRA sense) will acknowledge the fundamental principles of good risk governance and include them in recommended standards and guidelines.

7.6.1 Reconsidering the categorization of risks and risk problems

In the following, we will look more closely into some of the basic concepts of risk governance, as discussed in Section 1.6, in particular interpretative ambiguity, complexity, uncertainty, normative ambiguity and systemic risk.

Interpretative ambiguity

Consider first the interpretative ambiguity criterion. Think about the example discussed in Section 1.6.2 regarding neuronal activities in the human brain related to electromagnetic radiation. The issue is whether the change is to be interpreted as an adverse effect or just as a bodily response without any implication for health. When studying electromagnetic radiation, we

do not know what the consequences will be; there are uncertainties. Since knowledge can be viewed as justified beliefs (Section 2.2), the situation can be referred to as one with weak knowledge – and hence large uncertainties – as the justification for the specific statements (e.g. that the change is an adverse effect) is weak. The justified beliefs are in general founded on data, information, analysis, argumentation, testing, etc. ('evidence'). The knowledge search may never be conclusive; hence, the interpretative ambiguity will continue to exist.

In a risk context, we also need to relate this ambiguity, knowledge and uncertainty to impacts and consequences. Are the health effects minor or major? We see that we are led to considerations of risk, as defined in Section 4.2, which highlight two dimensions: (i) values at stake (the consequences of the activity related to something that humans value) and (ii) uncertainties (what will these consequences be?). There is risk associated with electromagnetic radiation; this risk is characterized by a potential for rather severe consequences, and there are considerable uncertainties about what the consequences will be. The risk is mainly due to interpretative ambiguity – we do not know what the neuronal activities in the human brain mean. The risk problem, electromagnetic radiation, is characterized by interpretative ambiguity.

Consider the risk characterization provided by a risk assessment for an activity (such as the operation of a technical system). Let us assume that the risk is described by the expected number of fatalities. There could be interpretative ambiguity related to this risk characterization, as there could be different ways of interpreting it. This applies to the meaning of the concept of the expected number of fatalities but also to the extent to which this concept actually describes risk for this activity. It is a generic issue, as discussed in Section 4.2 and Aven (2012a), but also a specific one related to the knowledge supporting the derivation of this number. It can be based on more or less strong knowledge (evidence), and just reporting the expected number of fatalities as a risk characterization allows for different interpretations of its strength and importance.

We can have a similar discussion if risk is characterized by consequences and probabilities (Aven 2012a); refer to Section 4.2. The point being made is that the risk characterization may allow for different 'goodness' interpretations. Key aspects to consider, when clarifying how to understand 'goodness', are the solidness of the assessment and the degree to which the assessment results are *reliable* and *valid*; refer to Sections 3.1 and 5.1. Poor solidness, reliability and/or validity may lead to interpretative ambiguity: different understanding of what the risk characterization expresses.

Suppose there is broad agreement that the risk characterization is informative and founded on seemingly strong knowledge. Then, there is no

interpretative ambiguity. Yet, the knowledge can be wrong – surprises may occur relative to the knowledge available. Hence, it is essential to see beyond the interpretative ambiguity when assessing a risk characterization. Consensus on the meaning and importance of the risk characterization is not enough. At one stage, all parties may agree on the information and strength of a risk characterization – there is no interpretative ambiguity, but additional research may lead to such ambiguity when new insights are gained.

Instead of referring to no interpretative ambiguity, one could choose to highlight the quality and goodness of the risk characterization, which include judgements related to the knowledge expressed by this characterization and its basis.

Complexity

Consider now the complexity criterion: it is difficult to accurately predict the system performance on the basis of strong knowledge of its individual components (Jensen and Aven 2018, SRA 2015a). In a risk analysis context, does this mean that there are large uncertainties (weak knowledge) about the performance of the system, that the problem is one of uncertainty, that is, that *it is difficult to accurately* predict the occurrence of events and/or their consequences?

Consider a complex system for which we have substantial statistical data on an overall performance level. From this basis, we may be able to make reasonably good predictions for the system performance; hence, there is not much uncertainty in that sense. There is always some uncertainty, as such data are historical and more or less relevant for the future; new types of events may occur, even if they have not happened up until now. As the system is complex, it is challenging to understand how it works and, further, how to improve it and avoid failures.

A common situation in practice is, however, that we have rather few relevant data available. Then, system performance needs to be analysed, and this is difficult for complex systems. Traditional methods are to a large extent based on the simple integration of individual components' performance. Tools designed for non-complex systems are often used (Hollnagel et al. 2006, Leveson 2011). The result is poor predictions and large uncertainties: the problem is one of large uncertainty. Other types of approaches and methods can be used – like FRAM (Hollnagel 2012) – yet the uncertainties remain large. The focus of these approaches and methods is typically more on how to best meet these uncertainties through robustness and resilience.

Uncertainty

Next, consider the uncertainty criterion. Suppose a risk problem is characterized as one with high uncertainty. Would it then deserve our attention? It

depends on the values at stake – the consequences. High uncertainty is only a problem if there is a potential for serious consequences of the activity. As we discussed in relation to the interpretative ambiguity criterion, we have a risk problem if there is a potential for serious consequences and the uncertainties are large.

How to best characterize the uncertainties is a debated topic of risk analysis. Two key points are being clear on what one is uncertain about and who is uncertain. Then, we need to be clear on what is a judgement made to describe the uncertainties (for example probability) and what is the knowledge on which this judgement is based. It is essential to acknowledge that this knowledge can be more or less strong, and even erroneous, and could be subject to further examination. Surprises may occur relative to this knowledge. The uncertainty judgement can be given considerable weight if the knowledge is strong but not if the knowledge is weak. Hence, risk problems characterized by large uncertainties mean more weight being placed on the knowledge characterizations than on just the probabilities; refer to the discussion in Section 4.2.

Normative ambiguity

Now some thoughts on normative ambiguity, which reflects the fact that there are different views concerning the values to be protected and the priorities to be made. This category is of a different type from those discussed above (interpretative ambiguity, complexity and uncertainty). The three other categories reflect features related to knowledge about the activity considered, whereas normative ambiguity concerns how we like/dislike or value these features. Thus, normative ambiguity extends beyond the scientific domain. We may all agree on the risk characterization in relation to nuclear energy but still have completely different perspectives and views on what weight we should give to the risks when making decisions on the use of this type of energy in a country.

The term 'ambiguity' can be understood as the condition of admitting more than one meaning/interpretation (SRA 2015a). In relation to the interpretative ambiguity criterion, this makes sense, as discussed above, but it is more questionable in relation to normative ambiguity, as the issue is not really about interpretation but how one gives weight to different concerns. Is the difference in political stands on various topics a question of interpretation? People and parties give different weights to the uncertainties in relation to the operation of nuclear power plants. Some accept the uncertainties because of the benefits nuclear power plants bring; others find them unacceptable. Clearly, the interpretation issue concerns not trying to find the meaning of the risk but, rather, the sense of understanding the significance or implications of the risk. The term 'ambiguity' can also be interpreted

in this way (Free 2018). There are different views on the significance and implications of nuclear activity and risks. This statement makes sense. The significance and implications relate to, for example, the uncertainties of experiencing major catastrophic events and how different concerns are balanced and valued.

Johansen and Rausand (2015) provide an in-depth analysis of the concept of ambiguity in risk assessment. They propose a new overall definition of ambiguity in the setting of engineering risk assessment: "Ambiguity: The existence of multiple interpretations concerning the basis, content, and implications of risk information". These authors define three types of ambiguity: "Linguistic ambiguity: A statement that can be interpreted in two or more possible ways; Contextual ambiguity: The existence of multiple contexts, premises, and knowledge relations in risk information; and Normative ambiguity: The existence of multiple, conflicting, and/or inconsistent values and norms in risk assessment". We interpret the first two as basically overlapping with the interpretative ambiguity criterion, whereas the normative ambiguity definition is different. In their understanding of normative ambiguity, Johansen and Rausand (2015) "focus on values and norms that govern the entire risk assessment process from preassessment to risk evaluation, but not the tolerability of risk as a balance between risk and other values (objectives) in decision-making".

Thus, these authors use the term 'normative ambiguity' in a narrower sense than in the IRGC tradition. Their focus is on risk assessment, whereas IRGC has a broader risk-problem perspective, capturing all aspects of risk management and governance. However, the delineation made by Johansen and Rausand (2015) is important – they avoid tolerability and acceptance of risk issues becoming a part of the normative ambiguity concept. Their definition of normative ambiguity can easily be made applicable for the broader context of risk management and governance (or risk analysis as used by SRA and in this book). Through their use of such an understanding of the concept, ambiguity is restricted to difference in interpretations and does not consider the significance and implications of the risks.

Systemic risks

Finally, in this section we look at the term 'systemic risk'. From the various sources describing systemic risk, it is not clear what this concept captures. In view of Renn's (2016) feature, "global in nature" (see Section 1.6), one may ask: are the only relevant risks those that have the potential to make the whole world or society collapse – seeing the world or global society as the 'system'? However, the term 'systemic' does not express that it is global *per se*; the system can be defined at different levels. We may have 'system risk' on a national level, for a municipality, or for an enterprise or company. It is, for

example, common for businesses and companies to talk about systemic risk. The term 'systemic risk', as defined by Kaufman and Scott (2003): "systemic risk refers to the risk or probability of breakdowns in an entire system", would still apply, but not if we require the concept to only relate to global threats. A possible reformulation of this definition is to say that systemic risk refers to the risk related to breakdowns of the whole system. Probability should not be used in the definition, as it is just one way of measuring or describing risk.

The definition of Kaufman and Scott (2003), with or without this reformulation, also expresses that the risk "is evidenced by co-movements (correlation) among most or all parts". This feature of the definition is further developed by Renn's (2016) second and third features of systemic risks: (2) highly interconnected and intertwined, leading to complex causal structures, and (3) nonlinear in their cause–effect relationships. However, Renn's features are not directly deducible from the definition of Kaufman and Scott (2003). Rather, features (2) and (3) can be viewed as ways of characterizing complex systems. This corresponds well with van Asselt and Renn's (2011) statement that systemic risks are *complex* and surrounded by uncertainty and/or ambiguity.

Renn's (2016) fourth feature states that the risks are stochastic in their effect structure. This can be interpreted as meaning that the risk problem is one of uncertainty, as *it is difficult to accurately* predict the occurrence of events and/or their consequences. It could also be understood as an expression that, for the activity considered, any dose/stress/load imposed on the system would have uncertain effects or responses.

Systemic risks are thus associated with the features complexity and uncertainty, as well as normative ambiguity, as this type of ambiguity is commonly a result of complexity and uncertainty.

7.6.2 Suggestions for alternative definitions and risk problem classification systems

In this section, we discuss some possible implications of the above findings. Should we perform a redefinition of key terms? Should some of the basic principles adopted be challenged? To provide an answer to these questions, we first need to clarify: what would we really like to achieve?

The classification systems aim at structuring and characterizing the risks and risk problems, to clarify what the essential features of these risks and problems are. This facilitates discussions of what constitute proper risk-management and -governance strategies, as different classes call for different strategies. The challenge is to balance simplicity in the classification system with the need to reflect the key features of the risks and risk problems. From the above analysis, we suggest a reformulation and simplification of

the current risk-problem classification system, as summarized in Table 7.2 and explained in the following.

Risk governance is to be understood as the application of governance principles to the identification, assessment, management and communication of risk, and it is thus a concept that applies to all types of risk and risk problems. However, its origin and common use relate mainly to more sophisticated types of risk and risk problems.

Of special interest are those risks for which there is (i) a potential for extreme consequences (for society) and (ii) large uncertainties concerning what will be the consequences. In such situations, the risks are to be considered high. The risk problem can be labelled one of uncertainty. If there is a relatively high probability of extreme consequences, and the knowledge supporting this probability is strong, the uncertainties are smaller, and the risk problem can be labelled 'simple'. Yet, the risk is considered large. Different management strategies are needed in these two situations.

Uncertainty could be a result of, for example, complexity or weak knowledge about underlying phenomena or processes (giving rise to interpretative ambiguity).

For a situation or risk problem, there are, commonly, different values related to the risk (consequences, uncertainties). The situation or risk problem can be labelled as one with 'value differences' or one of normative ambiguity using the IRGC terminology. There are, for example, nearly always different views on how much weight to give to uncertainties, relative to the potential benefits, in political decision-making processes. Differences in risk attitude or 'risk appetite' could explain the different views. Some are more willing than others to take on risky activities in pursuit of values. Today, many people and parties strongly prioritize activities and measures to protect the environment. Even in the case of quite small uncertainties, an activity cannot be justified if it threatens the environment. An example is the petroleum activities in environmentally sensitive areas in the Barents Sea–Lofoten area (Aven and Renn 2012). We find a similar attitude to risk and uncertainties in relation to nuclear energy. Other people and parties are more focused on the values that these activities can generate and, as long as the risks are not too high, they would like to carry out the activities. The priorities and risk attitudes differ.

The differences in values are influenced by many specific factors related to the consequences at stake. A structure for such factors is provided by the WBGU (2000); see also IRGC (2005) and Aven and Renn (2010):

1) Ubiquity, the geographic dispersion of potential damage;
2) Persistence, the temporal extension of potential damage;
3) Reversibility, the possibility of restoring the situation to the state before the damage occurred;

4) Delayed effect, which characterizes a long period of latency between the initial event and the actual impact of the damage;
5) Potential for mobilization, i.e. violation of individual, social or cultural interests and values, generating social conflicts and psychological reactions in individuals and groups who feel afflicted by the risk consequences.

The three main risk problems – simple, uncertainty and differences in values (Table 7.2) – call for different risk-management strategies. As commented in Sections 3.1.1, 7.1 and 7.5, there are three main categories of such strategies – risk-informed (using risk assessments), cautionary/precautionary (robustness, resilience) and discursive strategies. In practice, the appropriate strategy is a mixture of these three. However, there is a main strategy linked to each risk-problem class:

- Simple: risk-informed (using risk assessments),
- Uncertainty: cautionary/precautionary (robustness, resilience)
- Differences in values: discursive.

Systemic risk in this set-up can be understood as a risk related to a system, characterized by uncertainty and/or value differences. To highlight the system being addressed, reference should be made to global systemic risk, financial systemic risk, etc.

We may also use a term like 'non-simple risk problem' to refer to a risk problem characterized by uncertainty and/or differences in values, or simply state that the problem is one of "uncertainty or value differences", to avoid misinterpretations.

7.6.3 Final remarks

As discussed in Section 1.6, the risk governance literature can be viewed as a response to a situation with unsuitable frameworks and methods for handling today's public risks. The risks were treated, assessed and managed as if they were simple (van Asselt and Renn 2011). The then current assessment and management routines did not do justice to the type of risk involved. As this reference discusses, this situation has "sustained controversy, deadlocks, legitimacy problems, unintelligible decision-making, trade conflicts, border conflicts, expensive re-bound measures, and lock-ins" (van Asselt and Renn 2011).

Still, today, we see this happening: non-simple risk problems are treated as simple ones. This justifies the continuous focus on this issue and, hence, on risk governance. Although current risk-management and risk-analysis frameworks have been broadened to better understand, assess and handle non-simple risks, there is a strong need to highlight the features of non-simple

TABLE 7.2 A simplified risk problem classification system

Risk problem (situation) class	Description	Influencing factors	Main risk management strategies
Simple	'Objective' probabilities available		Use of statistical analysis and traditional risk assessments to guide decision-makers
Uncertainty	Case a: i) a potential for extreme consequences and ii) large uncertainties concerning the nature and the extent of consequences	• Lack of understanding of underlying phenomena • Complexity • Interpretative ambiguity	• Broad risk characterizations highlighting knowledge aspects and uncertainties • Weight on cautionary/precautionary/ robustness/resilience approaches and measures
Value differences	Case b I) a potential for extreme consequences and II) different values related to the risks (consequences at stake, uncertainties) Often the risk is one of uncertainty, but not necessarily (e.g. nuclear energy)	• Priorities • Risk attitude (appetite) • Ubiquity • Persistence • Reversibility • Delayed effect • Potential for mobilization	Participatory discourse; competing arguments, beliefs and values are openly discussed

risk problems and the related management strategies. Non-simple risk problems are challenging, and further developments on theory and practice are required. The risk-governance concept contributes to such developments by its framing and its focus on development and research.

The two dimensions, uncertainty and values, are key ones in decision-making where risk is an issue, and they have been previously addressed by many authors, including in the fundamental works by Fischhoff et al. (1981) and Stern and Fineberg (1996). Uncertainty has many interpretations, and it should be noted that uncertainty as here defined also relates to the consequences of the activity considered, as large uncertainty in itself is not necessarily a concern – unless there is a potential for severe consequences. Following the terminology in this book, uncertainty thus here refers to situations of high risk and uncertainty.

It is also interesting to compare the above risk-problem classification system with the Funtowicz and Ravetz model for classifying problem-solving strategies into applied sciences, professional consultancy and postnormal sciences (Funtowicz and Ravetz 1985, 1994, Aven 2013a), as mentioned in the Bibliographic Notes. The point being made is that, with high decision stakes and uncertainties, the situation is characterized as one of 'postnormal science', and different analysis and management strategies are required from those in the case of 'applied sciences' and 'professional consultancy'. We must see beyond traditional statistical data analysis and risk assessments. The risk-problem classification system of IRGC and the one presented in Table 7.2 can be viewed as an application and refinement of the underlying ideas of Funtowicz and Ravetz in a risk context.

A risk characterization informs decision-makers; it does not prescribe what to do (Apostolakis 2004). There is a leap – often referred to as broad risk evaluation or managerial review and judgement (Hansson and Aven 2014, see Sections 3.1.1 and 5.5.3) – between the assessment and the decision-making, which reflects that any assessment has limitations and there are concerns that extend beyond risk that are important for the decision-making. Risk governance and the framework presented and discussed in the present analysis provide a set-up for the proper recognition of this leap and the types of aspects that need to be taken into account to properly deal with it when making decisions under uncertainty and different values.

8 Solving practical risk analysis problems

This chapter examines some issues of importance for the practical use of risk analysis. First, we discuss certain challenges related to standards and guidelines. Section 8.1 studies the ISO 31000 standard on risk management, whereas Section 8.2 examines the guidance on uncertainty analysis produced by the European Food Safety Authority (EFSA). Then, in Section 8.3, a security risk analysis is presented, to demonstrate practical problems that analysts and decision-makers face when conducting risk analysis. Section 8.4 provides some reflections on climate change and risk analysis (risk science), many issues on this topic having been discussed throughout earlier chapters of the book. Finally, Section 8.5 makes some comments on training in risk analysis.

8.1 STANDARDIZATION: ISO 31000 ON RISK MANAGEMENT

There is considerable use of standards in industry and practical safety- and risk-related work today. We may question whether the standards actually enhance the risk and safety field, or do they in fact lead to the cementation of inadequate principles and methods? The literature covers many scientific works pointing to strong limitations and weaknesses in current standards (Tamm Hallström 2004, Timmermans and Epstein 2010, Rasche 2010, Tamm Hallström and Boström 2011, Brunsson et al. 2012, Wiegman et al. 2017), and experience indicates that it is difficult to influence the thinking supporting the standards. The processes involved in developing and maintaining standards like ISO 31000 are comprehensive, a result of international expert consensus and, as formulated by ISO, "therefore offer the benefit of global management experience and good practice" (ISO 2018).

However, does this consensus-driven approach actually deliver high-quality guidance, according to the best of the risk and safety fields and sciences? Do the standards favour compromise and the lowest common denominator of available options, at the expense of scientific quality? In this section, we examine this issue by comparing the highly influential ISO 31000 standard with the insights provided by risk science. We look specifically for lack of consistency and contradictions.

The ISO 31000 standard (ISO 2018) replaces the first edition from 2009. The main changes made in the new version are summarized in its foreword: a review is performed of the principles of risk management; the leadership by top management and the integration of risk management are highlighted, starting with the governance of the organization; and the iterative nature of risk management is given greater attention (ISO 2018).

The evaluation in this section is based on two overall criteria:

a) *solidness*, meaning that concepts are well-defined and coherent.
b) scientific knowledge of the risk analysis field.

What the scientific knowledge refers to will be clarified and discussed throughout the evaluation. Five main points will be highlighted in the following:

1) Overall features of the standard
2) Overall ideas linked to risk and risk characterization
3) Fundamental principles of risk management
4) The link between uncertainty, knowledge and information
5) Other examples showing lack of solidness

8.1.1 Overall features of the standard

Many features of the standard are non-controversial, and risk scientists would agree that they represent current knowledge of the field. On an overall level, the changes referred to above for the 2018 edition are unproblematic. For example, there is broad support for highlighting leadership and commitment in risk management. Again, on an overall level, there is broad agreement in the risk field that risk assessment provides a useful tool for informing decision-makers and other stakeholders about risk, and that there is a need for a structure and process for how to use risk assessments in risk management. There are many ways of describing this process, but they will all have features similar to those outlined in the standard. On a more detailed level, there are, however, many issues that could be discussed; see the coming evaluation. Also, the role of this process in risk management is a topic for debate; see Section 8.1.3.

The standard has a focus on objectives and meeting these, in line with the philosophy of management by objectives. It is a strongly debated philosophy, with some obvious strengths but also some severe weaknesses, as thoroughly discussed in the literature, particularly in the quality management discourse (e.g. Deming 2000, Bergman and Klefsjö 2003). Although the standard highlights continual improvement, the focus on objectives easily leads to a compliance regime, in which the main driver becomes task achievements, without really improving overall performance (Aven and Aven 2015).

The standard has a focus on organizations and their risk management. Certainly, aspects of the standard can also be useful for broader risk problems, such as global risks, but the scope of the standard is organizations (commercial, public sector and non-governmental) and their risk handling.

8.1.2 Overall ideas linked to risk and risk characterization

The standard defines risk as "the effect of uncertainties on objectives". In contrast to many other definitions of risk, uncertainty has replaced probability. The idea is in line with a recommendation made by the Society for Risk Analysis (SRA 2015a): we should not define the concept of risk using one specific measurement tool (probability). This is a basic principle of measurement theory: the concept should be distinguished from how it is measured. The idea is that we face risk when we operate a process plant or make an investment, independently of whether this risk has been measured or not. Certainly, probability is a main instrument for measuring or describing the uncertainties, but it has some weaknesses and there are also other approaches that can be used for this purpose. This idea is reflected in the ISO 31000 standard. Unfortunately, the standard is poorly formulated, as will be discussed in the following.

First, it is problematic that the risk concept is so tied up with formulations of objectives. We can question: does risk not exist if objectives are not defined? Think of some researchers who explore an unknown substance. Would it not be reasonable to say that they face risk? Yes, it would, despite the fact that an investigation objective has not been formulated. As another example, consider a case with many stakeholders having different interests and objectives. Some of these may be reluctant to express their preferences and goals. Yet, it should be possible to conceptualize and describe risk. Using the ISO definition, this is, however, problematic. In practice, risk assessment is commonly used as a means to develop formulations of objectives, by, for example, identifying factors contributing strongly to risk. However, the ISO conceptualization makes this impossible, as the objectives are incorporated in the risk term. Finally, think of an investor who invests an amount of

money in a specific project. The investor adopts a strategy in which he/she seeks to obtain as high a benefit as possible. He/she rejects the idea of formulating a specific objective. Then, risk as defined by ISO has no meaning, although intuition and common understanding of the risk concept would surely point to its existence.

Secondly, it is a problem that the ISO definition is so poorly formulated. To illustrate, consider the future realization of a specific activity. The outcome of the activity is either 1 or 0, corresponding to one fatal accident or no fatal accidents, respectively. We have formulated an objective as "no fatal accidents". Now, what is "the effect of uncertainties on objectives"? This is not clear. One possibility is that the statement expresses that the activity leads to a fatal accident and in this way does not meet the objective. However, such an outcome is not an effect of uncertainty but an effect (consequence) of the activity, and this effect (consequence) is uncertain prior to the realization of the activity. A note to the ISO definition of risk states that an effect is a deviation from the expected – positive, negative or both. Also, this is unclear: "the expected" – what does that mean? Think again about the 0/1 example. Suppose probabilities of 0.7 and 0.3 are specified for the outcomes 0 and 1, respectively. What, then, is the deviation from the expected – is it from 0 or from 0.3? The latter number is the statistical expected value of the probability distribution – the centre of gravity of the distribution. As a consequence, deviations from the expected could mean either 1 or 0.7. The main point being made, however, is not this lack of clarity related to the term 'expected' but that the deviation is not an effect of uncertainty – it is an effect (consequence) of the activity, and this effect (consequence) is uncertain prior to the realization of the activity.

Thirdly, it is a problem that the uncertainty characterizations pointed to in the standard are not really updated on current knowledge of the risk science. It is stated that risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood. Likelihood is then defined as the chance of something happening, "whether defined, measured or determined objectively or subjectively, quantitatively or qualitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period)" (ISO 2018). Likelihood is meant to be interpreted broadly, in contrast to a more narrowly interpreted mathematically based probability concept.

Likelihood is explained by introducing a new term, namely 'chance', which is not defined. The scientific literature provides clear definitions with interpretations; see, for example, Lindley (2000, 2006), Aven (2014b), SRA (2015a), and Appendix A. Why are these not used? The ISO text mixes underlying theoretical concepts – like frequentist probabilities – with estimates, as well as assignments of knowledge-based (subjective, judgemental)

probabilities. To characterize risk, it matters greatly whether we refer to an underlying 'true' probability, an estimate of this probability, or a knowledge-based probability, which is conditional on a knowledge base.

Certainly, likelihood (probability) is the most common tool for representing and expressing uncertainty, but the risk characterization should not be restricted to this measure alone. In relation to knowledge-based probabilities, there is, for example, a need to reflect the knowledge and the strength of knowledge on which the probabilities are founded. The ISO standard completely ignores this important aspect of a risk characterization. A considerable body of scientific literature argues for extended risk characterization, highlighting knowledge aspects beyond likelihood judgements (see e.g. SRA 2015a and Aven 2017c, and Section 4.2), but ISO 31000 is not updated on this matter. It refers to basically the same approach for characterizing risk as that in the 1970s and 1980s. The risk field has made many advancements, also related to interval (imprecise) probabilities (see e.g. Dubois 2010, Flage et al. 2014), but these are not reflected.

It is not realistic for us all to agree on one definition of risk. It is not needed. Nonetheless, it is both realistic and meaningful to seek broad agreement among risk assessment and management researchers and analysts, when it comes to the basic ideas of the risk concept and its characterization. As discussed in Section 4.1, risk captures two essential dimensions: (1) something is at stake – the activity considered results in some consequences with respect to something that humans value (including health and lives, the environment and material assets) and (2) uncertainties (SRA 2015a, Aven 2012a, Aven and Renn 2009). There are different ways of (a) conceptualizing this idea and (b) measuring or describing the risk and uncertainties, as shown in the SRA (2015a) Glossary and Chapter 4.

To characterize the uncertainty component, we are led to likelihood considerations (including intervals or imprecise likelihood judgements), knowledge characterizations, including judgements of the knowledge strength, and, finally, surprises relative to this knowledge. For the last element, the point is that there could be knowledge gaps, where we know little or nothing, or the justified beliefs that form the knowledge could actually be wrong. Potential surprises are, per definition, difficult to include in risk characterizations, but they need to be acknowledged as a risk source. Measures of different types can be implemented to meet this risk, for example implementing a qualitative analysis addressing such questions as (Aven 2014b, 2018e, refer also to Sections 4.2.4 and 8.3):

1. Has a risk assessment of the deviations from assumptions been conducted (an assumption deviation risk assessment)?
2. Have attempts been made to reduce the risk contributions from the assumptions that have the highest deviation risk?

3. Is the strength of knowledge, on which the assigned probabilities are based, assessed? Is this strength included in the risk description?
4. Have attempts been made to strengthen the knowledge where it is not considered strong?
5. Have special efforts been made to uncover potential surprises of the type, unknown knowns?
6. Have special efforts been made to uncover any weaknesses or holes in the knowledge on which the analysis group has built their analysis?
7. Have special efforts been made to assess the validity of the judgements made where events are considered not to occur due to negligible probability?
8. Have people and expertise, not belonging to the initial analysis group, been used to detect such conditions?

It is a research topic to improve current risk assessment practice to meet this challenge.

The ISO 31000 standard provides no discussion of issues like this. It is based on a traditional likelihood perspective on risk characterization, which has been shown to be inadequate for capturing all aspects of risk and uncertainties.

8.1.3 Fundamental principles of risk management

The ISO 31000 standard highlights eight principles, which are to be considered as the foundation for the risk management processes and frameworks. These principles are referred to as: integrated, structured and comprehensive, customized, inclusive, dynamic, best available information, human and cultural factors, and continual improvement. These all seem reasonable, but there is no reference to a rationale or argumentation for the selection of these principles. What is the scientific basis for the choices made? Many other principles could have been included. We would, for example, have given priority to a principle with a heading saying something like 'Risk science based', expressing that the risk management should aim to follow the guidance provided by the risk science. There could be ambiguity in relation to what this science states in some cases, but the statement is still relevant as a principle. It demonstrates a standard for the work: that it aims to follow the scientific knowledge of the risk science.

In addition to stating principles for the risk management process and framework, it would have been useful to formulate key principles for the risk management *per se*. It should be equally important to state what is good risk management, as well as good risk management processes and frameworks. The risk management process could be judged to be strong by reference to the ISO standard, but it completely fails if the reference is

the risk science. Examples of such principles have been developed by the Society for Risk Analysis (SRA 2017b). As an example, SRA (2017b) points to the need for using the following three main strategies for managing risk (refer to Sections 1.1, 7.1 and 7.5): risk-informed strategies (I), cautionary/precautionary/robustness/resilience strategies (meeting uncertainties, potential surprises and the unforeseen) (II) and discursive (III) strategies. In most cases the appropriate strategy would be a mixture of these three types of strategies. The higher stakes involved and larger uncertainties, the more weight on the second category and the more of normative ambiguity (different views related to the relevant values) the more weight on category III. ISO has published a guidance document on risk assessment techniques, but the point made here relates to the overall principles for how to scientifically best manage risk. The SRA principles guide users to seek the proper balance between strategies I–II. This type of guidance helps users to conduct good risk management, which is ultimately the aim of the standard. Such guidance should be essential for risk analysts and managers in their work, but the current version of the ISO documents lacks this type of support.

8.1.4 The link between uncertainty, knowledge and information

The concepts of uncertainty, knowledge and information are all referred to in many places in the ISO 31000 standard. They are all key terms in relation to this standard and risk management in general. However, none of them are defined or explained. Their interrelationship is not addressed or discussed. It seems that 'information' is more central than 'knowledge', at least if we are to give weight to the number of times these words are referred to in the standard.

As an example, the standard refers to "Best available information" as one of the risk management process principles, with the explanation: "The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders" (ISO 2018). Why not, instead, refer to 'knowledge' – and 'Best available knowledge'? Data and information provide input to the knowledge generation, and, by focusing on knowledge, a stronger statement is, in fact, obtained. Knowledge also captures beliefs justified according to scientific processes, using analysis, models, testing and argumentation. Reference is made to the well-established DIK (Data, Information, Knowledge) hierarchy (see e.g. Ackoff 1989, Rowley 2007, Zins 2007, Aven 2013d, 2014b).

The standard does not define or explain the uncertainty concept. The literature provides a huge number of definitions and classification systems

for understanding uncertainty, and it is unfortunate that the standard does not contribute to a clarification. Again, we refer to the Society for Risk Analysis and its glossary (SRA 2015a). As for risk, the glossary distinguishes between the concept and how it is measured or described. The qualitative concept captures the idea that a person does not know the true value of a quantity or the future consequences of an activity, for example to what degree an objective is met – that there is imperfect information and knowledge about the quantity or consequences. Different methods can be used to represent and express the uncertainties, including knowledge-based (subjective) probability (probability intervals) with related strength of knowledge judgements. The ISO standard provides no guidance on the issue whatsoever. In fact, it contributes to confusion with its notes on likelihood, which are inaccurate, and mixes underlying unknown quantities and the measurement of these quantities.

8.1.5 Other examples showing lack of solidness

Here are two examples to further demonstrate the lack of solidness in the standard. The first example is from Section 6.4.3 on risk analysis, where it is stated: "Highly uncertain events can be difficult to quantify" (ISO 2018). Yes, it is difficult to quantify events. Probably the intention was to say that it is difficult to quantify the risk associated with such events.

The second example is taken from Section 6.5.3 on preparing and implementing risk treatment plans. It is stated that the "information provided in the treatment plan should include: – the rationale for selection of the treatment options, including the expected benefits to be gained . . ." (ISO 2018). But why only *expected* benefits? Restricting attention to expected values could seriously mislead decision-makers. Uncertainty does not seem to be an issue. But it definitely is and should have been addressed in the text.

8.1.6 Some final remarks

There is considerable literature discussing the challenges of standardization; see for example the references mentioned in the introduction of this Section 8.1. The following measures should be considered for confronting the current situation and improving the risk and safety fields:

1) The ideal of consensus-building processes in standard-developing needs to be challenged. Rather, the ideal should be high quality, as judged by the scientific risk analysis community.
2) The scientific risk and safety organizations need to take greater responsibility as knowledge organizations and seek to influence the risk and safety fields on what represents high-quality risk analysis and management.

3) Regulators for different areas should give increased support to scientific organizations to build the organizational capacity to meet such a responsibility.
4) At the same time, the risk science community should increase its participation in standardization activities like ISO. It should build liaisons with the standardization organizations to influence the content and quality of the standards.

The ISO standards are developed through a multi-stakeholder process, and ISO highlights that they are established by consensus. However, this can be questioned. It can mislead potential users. It indicates that all relevant parties find the standard acceptable. This is surely not the case. As demonstrated by the above analysis, risk science has raised serious concerns about some main aspects of ISO 31000. As a risk expert, the present author does not find the ISO 31000 standard acceptable from a scientific point of view, and many of the arguments raised above have been presented to ISO but not taken into account. If we compare the ISO 31000 standard with the SRA Glossary and guidelines developed by the Society for Risk Analysis (SRA), there are several conflicting perspectives. Consensus is thus not established, if the reference is the broader community of professional societies and organizations working with risk. Within the formal processes of ISO, it can be argued that the processes are consensus-based, but consensus is only obtained because the processes are limited to some stakeholders and power is exercised. See Aven and Ylonen (2019) for further discussions of these points.

8.2 GUIDANCE ON UNCERTAINTY ANALYSIS

Scientific work, for example related to food safety, is about balancing confidence in the knowledge on how things are with humility, as there are limitations in this knowledge – there are uncertainties and risks; refer to the discussion in Sections 3.1.1 and 3.2.3. For example, research and testing may have shown that some specific food is safe, no serious negative health effects have been identified. However, the long-term effects may not be properly understood – there are associated uncertainties and risks. How should we deal with these uncertainties and risks? How should we conceptualize, analyse, describe, communicate and manage them?

The sciences of statistics, uncertainty and risk analysis and management should provide the answers. Unfortunately, they do not yet do this. There is no available authoritative guidance on these questions, the result being that different institutions and organizations develop such guidance themselves. An example is the guidance on uncertainty analysis produced by the European

Food Safety Authority (EFSA 2016). EFSA provides scientific advice on risks and other issues relating to food safety, to inform decision-making by the relevant authorities (EFSA 2016). According to this guideline, all EFSA scientific assessments must include consideration of all types of uncertainties.

The EFSA guidance does not specify which methods should be used; it is more a framework from which different methods can be selected. However, the framework is built on some fundamental ideas and principles; for example, it states that assessors should aim to express uncertainty in quantitative terms to the extent that is scientifically achievable, and probability is the preferred measure for expressing uncertainty.

The EFSA guidance will influence the way uncertainty analysis is conducted in scientific assessment, at least in Europe, and it has been given considerable attention by risk and uncertainty analysis experts. Recently, Löfstedt and Bouder (2017) and Sahlin and Troffaes (2017) provide interesting reflections concerning the EFSA guidance and related uncertainty analysis and communication in general.

The present discussion provides further analysis and perspectives on these topics. It is argued that the current EFSA guidance document provides valuable insights and recommendations concerning uncertainty analysis in scientific assessments but is subject to several severe weaknesses, which could seriously hamper effective implementation.

8.2.1 Fundamental concepts and ideas

Let us first examine the probability concept. The EFSA guidance states that "From the perspective of subjective probability it is always possible to quantify well-defined uncertainties" (EFSA 2016, p. 39). A proper definition of the concept with an interpretation is, however, not provided. It is stated that subjective probability means "quantification of uncertainty as degree of belief regarding the likelihood of a particular range or category" (EFSA 2016, p. 114). Bayesian probability and an operational definition of probability developed by de Finetti (1937) and Savage (1954) are referred to, but without explaining what they mean.

The meaning of probability needs to be made clear to effectively apply uncertainty analysis, but de Finetti (1937) and Savage (1954) do not provide the answers, as they mix uncertainty assessment and value judgements. Take, for example, the de Finetti interpretation, which, simplified, expresses that the probability of the event A, P(A), equals the amount of money that the assigner would be willing to put on the table if he/she would receive a single unit of payment in the case that the event A were to occur and nothing otherwise. In an uncertainty analysis, we expect the assessor to perform a pure uncertainty judgement, which is not influenced by his or her attitudes to the

gambling situation and the money involved; refer to the detailed discussion in Aven and Reniers (2013). The authors of the EFSA seem to be unaware of fundamental theories and practices of uncertainty quantification using probability: there is a well-proven way of interpreting a subjective probability, which is based on a pure uncertainty assessment: namely, the comparison approach, as presented in Section 3.1.1 and thoroughly discussed by Lindley (2006); see also Kaplan and Garrick (1981), Aven and Reniers (2013) and Aven and Renn (2015). The idea is as follows.

If an assessor assigns a probability of 0.3 (say) for an event A, he or she compares his/her uncertainty (degree of belief) in A occurring with drawing a red ball from an urn containing ten balls, of which three are red. The uncertainty (degree of belief) is the same. Such probabilities can be specified for all events A (provided that they are well-defined, it is possible to determine whether A occurs or not – there is no ambiguity).

Probability bounds (intervals), referred to in the EFSA document, can also be defined using this type of comparison. These bounds reflect imprecision, not uncertainty. If the assessor specifies an interval [0.1, 0.2], he or she is not willing to be more precise than this, given the information and knowledge available. The assessor expresses that the probability is higher than 0.1 with reference to the urn comparison, as in the example above, and lower than 0.2. Alternatively, we can express that the uncertainty and degree of belief is comparable to drawing a red ball out of an urn comprising 100 balls, of which 10–20 are red – the exact number is not specified. The EFSA document states that "Imprecision is a form of measurement uncertainty, due to variability in repeated measurements of the same quantity" (EFSA 2016, p. 32). This wording is not in line with established terminology in statistics and uncertainty analysis and confuses the reader. The EFSA document is not at all clear on the difference between uncertainty and imprecision.

The EFSA guidance acknowledges the subjectivity of the assignments and science in general; it states, as mentioned above, that subjective probabilities can always be determined for well-defined events. At the same time, in several places, the guidance refers to situations when the assessor cannot, or feels it is difficult to, assign probabilities. The language is somewhat contradictory. The problem lies in the lack of precision concerning what a probability is. It is stated that a probability is conditional on some knowledge and assumptions, but the implications for the assignments are not clear. Let A be the event of interest. Then we can write the probability of A as $P(A|K)$, stressing that the probability is in fact a conditional probability, given the knowledge K. For any well-defined event A, the assessor can assign a probability $P(A|K)$. However, when the knowledge is weak, the assessor may have difficulties in assigning the probability. The number seems arbitrary – a rationale for a specific number may be lacking. How should we then proceed?

One approach is to use imprecise probabilities (probability bounds), as also discussed in the EFSA guidance document. However, these intervals are also based on some knowledge and assumptions. As an example, consider a quantity x, which is assumed to have a value in the interval [1,3]; an expert states that 2 is the most likely value of x. No more information is available. This leads us to interval probabilities, as explained in Aven et al. (2014, p. 47), for example that $0 \leq P(x \leq 1.5) \leq 0.5$; see Section 4.2.2. Clearly, these interval probabilities are also conditional on some knowledge K, as it is assumed that x cannot be outside the interval [1,3] and the expert has based his/her judgement on some knowledge.

The next question is: what should we do about this knowledge K? It is related to either a precise or an imprecise probability assignment. The EFSA guidance does not provide clear answers. Qualitative uncertainty analysis methods are referred to, but these are not directly linked to the quantitative assignments. The key point being made is that a proper uncertainty assessment of an unknown quantity needs to cover three basic elements:

1) A measure of uncertainty (measure in a wide sense), typical probability (or probability intervals)
2) A judgement on the strength of knowledge supporting this measure
3) The knowledge with its basis

We refer to Section 4.2 for further discussion of the rationale for these elements.

Knowledge is a key concept in relation to uncertainty and uncertainty analysis, and it is unfortunate that the EFSA guidance does not explain what knowledge means, beyond writing a parenthesis following "knowledge" with the words, "evidence, data etc." The current version of the EFSA guidance lacks a platform such as 1–3, which can explain how different uncertainty analysis methods are related. Probability and strength of knowledge judgements, for example, work together: they are complementary. All quantitative uncertainty assessments should be supplemented with some type of judgement of the strength of knowledge supporting these judgements. On this point, the present EFSA guidance provides not clarity but confusion.

Any uncertainty analysis reflects the knowledge and beliefs of the assessor. The elements 2 and 3 aim at being clear on what defines this knowledge and how the assessor judges its strength. The knowledge (the justified beliefs) could be more or less strong – and even wrong. Is it beyond the scope of the analysis work to think about surprises relative to their knowledge and aspects that are unforeseen? The analyst's knowledge could be strongly dependent on an assumption, and deviation from this assumption could lead to surprises. Is this type of consideration not a part of the uncertainty analysis?

Such considerations should be an integral part of the analysis, as the issues are important for the decision-makers. The present EFSA guidance document does not, however, go into this type of discussion. This is considered a serious weakness of the document. It simply stresses that any quantitative analysis is conditional on some knowledge and some assumptions. The definition of a conditional assessment, stating that it is "an assessment which is made subject to specified assumptions or scenarios to address sources of uncertainty that have not been quantified", is unnecessarily narrow, as any analysis is a conditional analysis in the sense that it is based on some background knowledge.

Variation is carefully described in the EFSA guidance. However, unfortunately, the link to probability models is not very well explained. The EFSA Glossary refers to frequency-based probabilities: "the frequency with which samples arise within a specified range or for a specified category" (EFSA 2016, p. 114). This does not make sense. A frequentist probability of an event A is the fraction of times this event would occur if the situation could be repeated infinitely under similar conditions (see Sections 3.1.1 and 4.2). The frequentist probability is normally unknown and needs to be estimated. Probability models, like the Poisson model, are formed by families of such frequentist probabilities, generated by an unknown parameter. The distributions model variation in the phenomena studied. The EFSA guidance is not clear on these fundamentals, which form basic pillars for traditional and Bayesian statistical analysis.

Models play an important role in uncertainty analysis, and a key concept is model uncertainty. In the EFSA document, it is defined as "bias or imprecision associated with compromises made or lack of adequate knowledge in specifying the structure of a model, including choices of mathematical equation or family of probability distributions". This is not understandable. Simple and clear explanations exist; see Section 5.3.

The EFSA guidance document does not include fuzzy-based methods (EFSA 2016, p. 76). The argumentation used, is, however, not very convincing. Fuzzy-based methods are many things. The above example, with x being an unknown quantity of the interval [1,3], leads to possibility theory and probability bounds, which are adopted in the EFSA guidance document. However, the use of fuzzy probability to reflect ambiguous statements (like "few failures") is another issue. Strong arguments can be raised against such probabilities, as no meaningful interpretation can be provided. Authors such as Bedford and Cooke (2001) reject such probabilities, as does the present author. The point being made is that, for any concept to be used for uncertainty characterization, it needs to be defined in a precise way. We can always include information that is vague and imprecise in the analysis, as a part of the background knowledge for the assignments we make. However,

the quantity of interest needs to be well defined, having some true underlying values that can be meaningfully specified.

8.2.2 Uncertainty analysis and risk

EFSA's guidance is closely linked to risk assessment. A main goal of the guidance is to characterize in a harmonized way the underlying uncertainties in EFSA risk assessments (EFSA 2016, p. 19). The guidance captures all types of scientific assessment, but risk assessment is clearly the central one. However, the guidance document does not define what risk is, although the term is used in many places in the document. It is a serious weakness of the document that the relationship between uncertainty analysis and risk is not clarified. Löfstedt and Bouder (2017) provide some perspectives on risk in this context, and these will be examined further in the following.

In the EFSA document, uncertainty "is used as a general term referring to all types of limitations in available knowledge that affect the range and probability of possible answers to an assessment question" (EFSA 2016, p. 20).

But what are the assessors uncertain about? This is a key question, but not one that is really addressed in the EFSA document. Basically, in this context, we can be uncertain about (Aven 2014b):

i) The future, what will the consequences of the activity studied be?
ii) Unknown quantities, including parameters of models.

Risk assessment deals with both. Consider a situation where the quantity of interest is the number of people in a population that will experience health problems due to a specific substance. We have limitations in the knowledge concerning what this number will be. Thus, uncertainty analysis is needed. However, we could also say that the situation calls for a risk assessment, as risk assessment is the tool to be used for studying the risk related to health problems caused by this substance.

If, on the other hand, a probability model has been developed, representing the fraction p of people in the population who will suffer health problems, the uncertainty analysis would address limitations in the knowledge of p, as well as model uncertainties. A risk assessment needs to include such uncertainty studies if risk is to be properly analysed.

The EFSA guidance document provides no reflections on issues such as these. How then can people be guided in using uncertainty analysis in a risk assessment context?

The risk analysis science is developing, and current thinking sees uncertainty as a key component of risk (refer to Section 4.1). Risk has two main elements: (i) the values at stake, consequences with respect to something

that humans value, and (ii) uncertainties. Uncertainty analysis thus needs to be an integral part of risk assessments, and guiding people on uncertainty analysis in a risk context without also describing the risk fundamentals is not very informative.

In its most general form, risk assessment recommends uncertainty assessments of the form (Q,K), where Q is a measure or description of uncertainty and K is the knowledge supporting this measure. Combining (Q,K) with the specified consequences of the activity considered, a risk characterization is obtained; refer to Section 4.2.2.

This leads us to the discussion in the previous section, where an argument was made for using probability (probability intervals/bounds) and related strength of knowledge judgements to describe these uncertainties; that is, Q is equal to probability (probability intervals/bounds) plus strength of knowledge judgements.

Situations with large or deep uncertainties are of special interest. They mean that the related knowledge is weak. In the EFSA guidance document, deep uncertainty is defined as "a source or sources of uncertainty, the impact of which on the assessment the assessor(s) is not able to quantify" (EFSA 2016, p. 113). This definition is unclear, in view of the fact that we can always quantify subjective probabilities (for well-defined events). See also Cox (2012), Aven (2013b) and Shortridge et al. (2017) for in-depth discussions on the concept of deep/large uncertainty, with a link also to the precautionary principle. The perspective taken is that we have scientific (deep) uncertainties (the trigger or criterion for the invocation of the precautionary principle) if we cannot establish an accurate prediction model for the phenomena studied.

The weaker the knowledge, the larger and deeper the uncertainties, the less weight can and should be given to the probabilities and the uncertainty quantification, as their basis will be poor. Then, the challenge is to describe or characterize the knowledge and uncertainties, by for example (partly based on Hansson and Aven 2014):

- Summarizing and reviewing the knowledge (justified beliefs) and its basis: data, information, testing results, modelling insights, argumentation, etc.
- Reporting signals and warnings indicating the occurrence of events, including 'emerging risks' (we say that we face emerging risk related to an activity when the background knowledge is weak but contains indications/justified beliefs that a new type of event could occur in the future and potentially have severe consequences for something humans value (Flage and Aven 2015)).
- Characterizing the robustness of systems and their interactions.

- Analysing alternative scenarios, including scenarios with events regarded to be implausible.
- Studying successes and failures in previous responses to surprising and unforeseen events.
- Developing, analysing and measuring generic abilities that are considered necessary in the response to a wide range of surprising and unforeseen events.

This also means the use of qualitative methods. The limitations of such methods are well known, but there is no alternative and, for sure, such methods can provide useful decision support, as also acknowledged by the EFSA guidance document.

8.2.3 Communication and decision-making

EFSA has a clear mandate, to "be an independent scientific source of advice, information and risk communication in order to improve consumer confidence" (EFSA 2016, p. 101). Uncertainty analysis plays a key role in EFSA's work. As stated in the abstract of the guidance note: "To meet the general requirement for transparency in EFSA's work, all its scientific assessments must include consideration of uncertainty. Assessments must say clearly and unambiguously what sources of uncertainty have been identified and what is their impact on the final assessment outcome: what range of outcomes is possible, and how probable they are."

The EFSA guidance document discusses rather thoroughly the dilemmas in risk and uncertainty communication. The desire for confidence – that for example the food is stated as safe – must be balanced against the desire for transparency and communication of the uncertainties. The document acknowledges the need to tailor the communication to different target groups, yet the overall aim is to reveal all relevant uncertainties in scientific assessments. Löfstedt and Bouder (2017) make some in-depth reflections on this policy and the EFSA communication strategy in general. Starting from a discussion of the scientific insights provided by the risk communication literature, the authors express some concerns that EFSA may lose some public trust by acknowledging and highlighting uncertainties. The discussion is followed up by Sahlin and Troffaes (2017), who seem to consider these concerns problematic. Their view is that the way forward is simply to become better in uncertainty analysis, and the EFSA guidance provides a useful platform for this.

Certainly, communication of risk and uncertainties involves a dilemma, as described above. However, the present author agrees that there is no alternative to transparency and openness when it comes to uncertainties

and risk in the context here discussed. How can we trust the authorities if we know that they are more concerned about avoiding stress and panic than revealing the uncertainties and risks? Today, people seek the best data, information and knowledge available. Public authorities would quickly be in trouble if they thought more about camouflaging these uncertainties and risks than acknowledging and dealing with them; refer also to the discussion in Section 6.2.3.

The issue is, rather, how we should perform the uncertainty and risk analyses, as commented by Sahlin and Troffaes (2017). Current practice is simply not good enough, as the analysis in this Section 8.2 indicates. People are not properly guided on how to conduct uncertainty analysis. A main problem is that the fundamentals are not in place: for example, the understanding of what a probability means. How is it possible to meaningfully communicate uncertainty and risk, when an interpretation of the most basic tool – probability – is not available? It is simply not possible. It will fail. Successful communication of risk and uncertainties requires a proper scientific platform (refer to discussion in Section 6.2). Unfortunately, such a platform is missing in the EFSA guidance document.

The discussion in the previous sections has pointed to some of the pillars of such a platform. To illustrate some implications for communication and decision-making, take an issue related to what is safe food. In a particular case, the food may be judged as safe if there are no unacceptable risks. That could be operationalized by saying that the food is safe if:

a) the judged probabilities of undesirable events (suitably defined) are sufficiently small, and
b) the knowledge supporting the probabilities is sufficiently strong.

What is 'sufficient' here is a management issue and not for the analyst and analysis to determine. It does not need to be a specified numerical quantity. Qualitative criteria and processes can be used, including deliberation and discussion of all relevant aspects, as is common in scientific committees.

If a or b or both are not met, the food is not considered safe.

This example demonstrates how the uncertainty analysis provides input to the communication and decision-making, by highlighting probability, for which a simple clear interpretation is provided (see Section 8.2.1), and the judgement about the supporting knowledge, which is linked to data, information, argumentation, testing, modelling, etc.

Both Löfstedt and Bouder (2017) and Sahlin and Troffaes (2017) argue for new approaches for uncertainty analysis. Löfstedt and Bouder (2017) argue that uncertainty should be seen as an integral part of risk – to avoid "over-precautionary" biases, which the present author interprets as

uncertainty being given too much weight in the relevant communication and decision-making processes. These ideas are in line with the argumentation provided in this book; see also recommendations in Aven (2010a), where uncertainty analysis is linked to risk assessment.

8.2.4 Conclusions

There is a strong need for guidance on how to conduct uncertainty analysis in scientific assessments. The EFSA guidance document provides many relevant and important discussions and recommendations to this end, but, unfortunately, it suffers from several weaknesses, which have serious implications for its successful use. The present discussion has pointed to some of these. The key message is the following:

1) The document lacks a proper foundation that clarifies the meaning of key concepts. The most central concept, probability, is not properly defined and explained.
2) There is a lack of structure that can bring clarity to the analysis and its use. Such a structure needs to clarify and explain what we are uncertain about; the two complementary building blocks: judgements of probability (probability bounds) and the knowledge supporting these judgements; and probability models representing variation.
3) A clarification of the relationship between uncertainty analysis and risk is lacking. Using current frameworks for risk conceptualization and assessment, uncertainty analysis is an integral part of risk analysis.
4) Having established a solid platform for uncertainty analysis, as outlined by these points and in greater detail in previous sections, improved communication and management of uncertainty and risks can be obtained, as sketched in Section 8.2.3. There is no alternative to an open and transparent strategy for authorities to deal with uncertainties and risk, if we would like to live up to the ideals of our modern societies.

Improvements are needed to rectify these problems. A basis for how to carry out such improvements has been outlined in the above analysis and throughout this book.

8.3 A SECURITY CASE

This section provides some reflections on how managers should think about risk when facing challenging decision-making situations with large uncertainties and high values at stake. A security case taken from the oil and gas industry is used to illustrate the discussion.

Back in 2003, the Board of Directors of the Norwegian oil company, Statoil (now Equinor), made a decision to acquire 50 per cent of BP's interest in the In Amenas project in Algeria. Statoil's global footprint and experience base at the time was rather limited, and this acquisition represented a major move, subject to high risk and a new type of risk events. The major operational risk identified and discussed in the time prior to the decision was the security risk for personnel, both at the gas facility and in transit between the gas facility and the airport. Algeria had just come out of a decade of unrest, and kidnapping by terrorists for ransom was not unheard of. Reassured by having BP and Algerian Sonatrach as partners with global and local experience, and by relying strongly on the Algerian military for protection, the decision to invest was made. The security was found to be satisfactory. In other words, the risk of terrorist attacks was found to be within company standard and conduct – assuming the army would protect the facility and the workers from terror. This assumption was considered to be solid, as the Algerian government was heavily reliant on the income from the oil and gas industry. The strong track record for the Algerian army demonstrated this. The assumption failed, as there was a surprise attack in the early morning hours of 16 January 2013. It became one of the largest terrorist attacks in the history of the industry. The number of innocent humans losing their lives reached 40, in addition to 29 terrorists killed (Statoil 2013).

In the aftermath, it seems obvious that the assumption and background knowledge should have been better analysed and given weight in some way. The current analysis is based on the thesis that managers are well qualified to understand and manage risk and uncertainties, but that there has been a lack of suitable conceptual frameworks available that adequately address the knowledge dimension. It is, for instance, common to consider risk to contain a combination of consequences (loss) and probabilities, which pays little attention to the knowledge base, including the assumptions underpinning the numbers, as has been thoroughly discussed in the present book (see e.g. Section 4.2). Changed assumptions can lead to quite different numbers. The risk, uncertainty and potential for surprises associated with this knowledge base need to be addressed and given weight to in some way. Giving weight to risk, uncertainties and potential surprises, in synthesis and balance with other concerns, is primarily the responsibility of the managers, though risk analysts need to contribute to the analysis part, informing the managers.

8.3.1 A thought-construction, going back in time: The request for a risk assessment

Let us turn back in time to 2003 and take the stand of a manager. Assume an investment opportunity – the In Amenas project – has been presented.

At first glance, it seems like a good fit for Statoil's strategic ambitions. The decision problem is whether to invest here or in other alternatives, including waiting for a potentially better option, but also whether controlling actions should be taken in the case that an investment is made. The investment prospect will ordinarily only be chosen if it represents a good/best means to achieve the strategic objectives of the company, including to maximize profits and ensure security for the personnel. Identifying good alternatives may be time-consuming and not straightforward.

In Amenas is located far away from home, not only geographically speaking. Algeria has had unrest lasting for a decade that has just come to an end, but terrorist groups are still active. Undoubtedly, there are opportunities that may pay off very well for those who dare, but there are uncertainties, and there may be large negative surprises hidden in the future. There is risk; and an analysis of risk is in place. To provide support with this task is the job of the risk analysts, and their services are requested.

First, a manager needs to reflect on what information the analysts should provide. What is important and useful to know, in order to make the decision? Financial risk obviously, but security risk is also important in this case given the presence of terrorist groups and the recent political unrest. Other aspects are also important, but we focus here on these two. Secondly, and most importantly, attention must be devoted to uncertainty, knowledge and potential surprises (black swans) in relation to these two: finance and security. A manager and leader should motivate, facilitate and request this from the risk analysts. One way to do this, for financial risk, focusing on the cost side, is to request expected values (best estimate) and some type of uncertainty intervals. In this case, say that the In Amenas expected project cost is estimated at \$750m. A 90 per cent uncertainty interval within which the analyst believes the 'true' cost will lie, say \$[600,1500]m, is informative. It is equally important to request an accompanying assessment of the strength of the knowledge underpinning all these numbers. One way to assess the strength of the knowledge is to use a scoring system, as presented in Section 5.5.3.

To exemplify, the strength of the knowledge underpinning the expected cost could be judged poor. One reason is very limited data on how well local workers and contractors will comply with formal contracts. Experts point out that this has been an issue elsewhere in the non-Western world because of cultural differences. The issue has caused costs to rise beyond projections for many projects and is not accounted for in the estimate. New assumptions and an update of the estimate using these assumptions could be made, but the strength of the background knowledge would, however, still be poor. Similar strength of knowledge considerations can also be made for the assigned uncertainty intervals.

Next, key assumptions must be made visible for scrutiny about their importance. Assumptions are normally identified and written down along the budgeting process. There are also structured techniques to make assumptions visible. For instance, Dewar (2002) presents nine techniques. One of the techniques is Discovery-Driven Planning, which aims at new business ventures facing pervasive uncertainty such as the potential move to invest in In Amenas was for Statoil. Assumptions in the budgeting are captured through a reverse income statement and pro forma operations specifications. The reverse income statement starts with required profits and works backward to set necessary revenues and maximum costs, in order to obtain the profits. This again determines the required specifications on production, shipping, equipment, and so forth, in this case for the In Amenas. The specifications then become the assumptions for achieving profitability.

Once key assumptions are identified, their importance can be assessed in greater detail. One way to do this is to assess the assumption-deviation-risk (Aven 2013e; see also Section 4.3), i.e. analysing what deviations from the assumptions could occur and what consequences such deviation would have for the cost. This could be performed by considering (1) the magnitude of a potential assumption deviation, (2) how likely the deviation is, (3) the consequences given a deviation, and (4) the strength of knowledge supporting the likelihood judgements. It can, for instance, be planned/assumed that the project period is 24 months. What happens to the cost if the actual project period deviates from this assumption and is doubled or tripled, due to engineering challenges? How likely are these outcomes, what are the consequences for the costs and what is the strength of the knowledge underpinning these judgements? The knowledge description is particularly important when the knowledge base is poor.

In addition, evaluations of potential surprises (black swans) should be requested. Assessment and judgements should be made for:

1) Potential thematic knowledge not possessed by the risk analyst group, in search for potential black swan type 'unknown knowns' (refer to different categories in Section 4.2).
2) Evaluation of events judged negligible due to low probability. This can include looking into historical events and experts not following the dominant way of thinking, and scrutinizing assumptions made.
3) Evaluations of weaknesses and gaps in the underpinning knowledge K.
4) Evaluations of how stable the knowledge and assumptions are considered to be over time.

When it comes to security, the request should not only cover scenarios, probabilities and expected consequences, given an attack, or quantities like

individual risk (IR), fatal accident rate (FAR), potential loss of life (PLL), f-n curves etc., but also, and equally importantly, ensure that the background knowledge underpinning these numbers is assessed in the same way as for financial risk. Take, for example, the assumption that the military will prevent terror – what if it fails? What could be the consequences? An assessment of the assumption deviation risk needs to be requested.

It is essential to highlight how the knowledge and assumptions concerning security and terrorism can change very rapidly and are directly life-critical, as opposed to the case for cost. Information about the changeability of the knowledge is vital for decision-makers to make an informed decision. A structured way of monitoring and tracking critical assumptions would be useful; cf. Dewar (2002). Continuous knowledge acquisition and intelligence for updating the status would be necessary.

Table 8.1 below summarizes the request. The request can cover alternatives other than to invest in the In Amenas project, also, as highlighted before, the alternative of not investing at all. A comparison can then be made between the alternatives, which focuses on knowledge, uncertainties and black swans.

In the search for potential surprises (black swans), it is essential that the existing knowledge is scrutinized and other sources of knowledge accessed. In practice, this means that not only self-critique is mandatory. It is also essential that people with other competences be brought in to have a critical and independent view of the risk analysis. Structured techniques to assist in the processes can be found, for instance within the intelligence community, through a family of techniques known as Challenge Analysis or Alternative Analysis; see, for example, Fishbein and Trevorton (2004), and Heuer and Pherson (2010). Essentially, these methods are trying to challenge assumptions and expand the range of possible outcomes in existing analysis (Fishbein and Trevorton 2004).

One way of performing structured self-critique is by what Heuer and Pherson (2010) refer to as Premortem Analysis. The analysis starts by imagining a future point in time at which the current assessments would be judged wrong or poor, and then imagines what the cause of the poor assessment is. Take, for example, the assessment that a terrorist attack is improbable, and the strength of the background knowledge is strong. Imagine that, at some future point, a terrorist attack is very probable and/or the background knowledge poor. What could have caused the poor assessment in the first place? The following subquestions constitute a good starting point to answer this (adapted from Heuer and Pherson 2010):

- Were important areas of thematic knowledge not covered?
- Did external influences affect the outcome?
- Were sources of data and information unreliable?

TABLE 8.1 Summary of the risk analysis request, covering different aspects and alternatives (based on Bjerga and Aven 2016)

Alternative Attribute	1: Invest in In Amenas	2: Second alternative	n: nth alternative
Cost	(Best) estimates		
	90% uncertainty intervals*		
	Strength of knowledge assessment		
	Key assumptions identification		
	Assumption deviation risk assessment		
	Evaluations to reveal potential unknown knowns, i.e. knowledge about the topic not possessed by the group but which others may possess		
	Evaluations of events judged to not occur due to negligible probability		
	Evaluations to reveal potential weaknesses and gaps in the knowledge underpinning the risk analysis		

Security	Scenarios/consequences
	Probabilities
	Strength of knowledge assessment
	Key assumptions identification
	Assumption deviation risk assessment
	Evaluations to reveal potential unknown knowns, i.e. knowledge about the topic not possessed by the group but which others may possess
	Evaluations of events judged to not occur due to negligible probability
	Evaluations to reveal potential weaknesses and gaps in the knowledge underpinning the risk analysis
	Evaluations of the changeability of the knowledge

. . .

[*] An x% uncertainty interval is an interval that the assessor believes will contain the 'true' number, with x% probability. This probability is to be understood as a knowledge-based probability, interpreted using a reference system: For example, 10% confident is comparable with drawing one favourable ball out of an urn containing 10 balls; refer to Sections 3.1.1 and 4.2.

- Did deception and biases go undetected?
- Was any contradictory information or expert ignored?
- Did the absence of data/information mislead us?
- Were our key assumptions reasonable?

For structured critique by others, different techniques, such as red teaming, exist. A red team is an analysis team, consisting of members from outside the original analysis team. Their task would be to take the side of an opposing view. The red team could, for example, argue for the occurrence of rare events, like a terrorist attack, look for holes in the knowledge, and check how precursors and warnings have been dealt with. For security and the potential for terrorism, experts on Algeria, experts on terrorism and military personnel would be natural candidates for such a group, if not already in the first group.

In this case, it might also be interesting to consider protection measures to reduce the risk, for instance in case the Algerian military forces fail to prevent terrorist attacks. It is common to use cost-benefit type of analysis, based on the expected net present value formula (E[NPV]), or calculations of the implied cost per averted fatality (ICAF) in such cases. Again, the uncertainties, strength of knowledge and potential surprises must be assessed in a similar manner as above, since expected values and probabilities alone are not sufficient to reflect risk; refer to the discussion in Sections 4.2 and 7.2.

In accordance with the request, the risk analysts will conduct the analysis and return a risk description. The risk description covers requested information and knowledge in relation to the risk, assessed through the eyes of the risk analysts and experts.

8.3.2 Managerial review and judgement focusing on knowledge and surprises

The manager conceptualizes risk as (C,U): investing in Algeria has some actual consequences, but these are uncertain/unknown at the decision point. The risk description handed over targets this risk, but has limitations, even when the analysts have assessed the background knowledge. There can still be surprises hidden that require attention and consideration. The manager needs to make his/her own judgement, reflecting on the numbers, knowledge assessments and surprise assessments made by the analysts. One way of doing this is by a similar approach to that of the 'red team' introduced above – taking an opposing view. The same points (1) to (4) need to be evaluated by the manager: what if large terrorist groups should reach the facility? What are the limitations of the probabilities derived? What if the military turn their guns? What would weaken the government's incentives to protect the facility? The knowledge base needs to be scrutinized and critical questions asked.

There are also other related concerns, for example that the risk analysts themselves might be 'biased'. For instance, could the risk analysts have personal interests in a decision to enter In Amenas or in a particular security technology? This issue is often seen in political decisions. Administrative staff perform the analysis, prepare the case and advise the elected officials on a decision. Of course, the administrators try to be objective in their assessment, but they too have political or financial interests of their own, which may influence the analysis and advice. The manager must also take similar concerns into account, when presented with a risk description, as such 'biases' could lead to unpleasant surprises.

Also relevant is the fact that the risk analysis with its limitations is only one contribution of many. The risk description only targets some aspects and events. In this case, only finance and security risk are considered. What about technical challenges? Or third-party risk? Or the environment? There might also be interdependencies between security and finance not sufficiently highlighted. The manager must also bring these elements to the table.

A decision is risk informed, not risk based in the sense that the risk assessment prescribes what decision is to be made, as highlighted in Chapter 7. The risk description will only target some aspects and events and has weaknesses and limitations in both its quality and scope. Table 8.2 below is a checklist, which summarizes the essentials of what the manager should take into consideration.

TABLE 8.2 Checklist for managers (based on Bjerga and Aven 2016)

Has the strength of knowledge been assessed?
Have key assumptions been identified?
Have key assumptions been assessed? (assumption deviation risk)
Is a monitoring programme of key assumptions in place?
Are the limitations of the uncertainty description considered?
Has the analysts' competence level been assessed and accounted for?
Has the risk analysis team performed self-critique of the analysis, to identify potential surprises? (e.g. premortem analysis)
Has independent critique of the risk analysis been performed, to identify potential surprises? (e.g. red teaming)
Have identified potential surprises been dealt with?
Have manager(s) performed a critical review?
Have potential biases been accounted for?
Have interdependencies between attributes been accounted for?
Are missing attributes accounted for? (e.g. the environmental impact)
Have third party risks been accounted for?

8.3.3 Giving weight to uncertainties and potential surprises in the decision

At the point when the risk description is judged eligible to be input to the decision, and all elements are on the table, the next role of the manager begins: to give weight to consequences and potential surprises, uncertainties and knowledge in balance and synthesis with other concerns. Many principles are applicable to that end.

Giving weight to uncertainty is giving weight to principles like the cautionary and precautionary principles (see Section 7.3). In the In Amenas case discussed here, there are large uncertainties and poor knowledge, and both principles can apply. This could mean that the investment is not made or that further measures to reduce risk are taken. Some potential candidates to reduce the risk for terrorist attacks would be to hire more security personnel, arm the security personnel, invest in intruder-safe shelters, put greater effort into training in the case of emergencies, and surveillance. The degree of caution taken needs balancing against attributes like cost, and they all come with security risks of their own. For instance, arms given to security personnel can potentially also be used against the personnel they are supposed to protect.

In line with cautionary thinking and the case when the question is whether or not to implement an identified mitigating measure, like armoured shelters designed to withstand a terrorist attack, the ALARP principle might be used (see Section 7.3). For the manager, it means that the risk should be as low as reasonably practicable, where 'reasonably practicable' needs to be seen in relation to other costs and benefits. The ALARP principle means a reversed burden of proof, i.e. identified reducing measures shall be implemented unless gross disproportion between cost and benefits can be demonstrated. It is common to use a cost-benefit type of analysis, as mentioned in Section 7.3, for such demonstration. However, when giving attention to uncertainties and potential surprises, a decision cannot be made based on the expected numbers alone. This especially concerns the cases when the cost is high and the cost-benefit analysis demonstrates gross disproportion. Still, the measure should be considered to be implemented if the strength of knowledge is poor, provided it can strengthen knowledge or the measure will reduce the risk of surprises and black swans. Refer to the discussion in Section 7.3.

It is also common to use risk acceptance criteria. If the risk is below a predefined limit, then the risk should be accepted, as discussed in Section 7.1. Care needs to be shown when using this type of approach. Weight must be given to knowledge, uncertainty and potential surprises and not only calculated probabilities. In cases of poor knowledge, the use of probability-based criteria cannot be justified.

Another way to give weight to potential surprises is to give weight to resilience, as thoroughly discussed in Section 7.4. In practice, there is always a trade-off between resilience and efficiency, i.e. how much weight and how many resources the manager is willing to give resilience.

8.3.4 Discussion

The example in this Section 8.3 has illustrated some managerial issues linked to risk assessment and management. It is underscored that the managers need to see beyond the conditional risk description, as described by (C',Q|K), as K may conceal important aspects of risk that should be taken into account in the decision-making; refer to Section 4.2.

There are various tools and measures applicable for carrying out the evaluations of these elements. For the risk characterization (C',Q), and security in our case, scenarios, probabilities and expected consequences were requested. Best estimates and uncertainty intervals served the same purpose for finance. Other measures like imprecise probabilities could also apply. From a practical point of view, it may be preferable to use the same way of measuring aspects, for all alternatives, as this would make comparison fairly straightforward. Equally important are the qualitative aspects linked to the analysis of the knowledge and the unforeseen. Potential surprises of the type 'unknown knowns' and 'ignored due to very low judged probability' (refer to Section 4.2) can be dealt with to some degree by means of scrutiny and knowledge sharing/transfer. The knowledge exists; it is just a matter of finding it or using it the right way. That is what one would do when performing self-critique, employing a red team or hiring specialists. It is also the same thing a manager would do when using his/her knowledge to review the work done. 'Unknown unknowns', however, are by definition very hard to do something about (unknown to the entire scientific community). Fortunately, knowledge is changing and growing with time, so that what is unknown at the current time may not be unknown at a future point in time. Research and development can reveal potential unknown unknowns. In addition, there are often signals and warnings, also for this type of events. Paté-Cornell (2012) recommends a mix of alertness, quick detection and early response to cope with unknown unknowns, but this also applies to the other types of surprises.

8.3.5 Conclusions

The above discussion has primarily been concerned with how managers should think about risk and what techniques and principles they should apply in related decision-making. The work is based on the thesis that there has been a lack of suitable conceptual frameworks to account for the

knowledge and surprise dimensions of risk. A decision process case from the oil and gas industry has been used to exemplify various aspects of how to account for these dimensions. At the very centre is the way risk is understood, and the request/description of risk it leads to, which addresses specified consequences and measures of uncertainty, assessments of underpinning knowledge, and surprises relative to the knowledge. It is argued that the cautionary principle needs to play an important role in the decision-making, to give proper weight to the uncertainty component of risk. The management task is to balance different concerns, such as security/safety and costs, but, in order to do this in a meaningful way, the full spectrum of the uncertainty dimension must be reflected. The present analysis has pointed to some key aspects to consider, which extend beyond current practice.

8.4 CLIMATE CHANGE RISK

In this section, we discuss how the field and science of risk analysis can support climate change management and governance. The topic of climate change is concerned with how the climate is changing over time, what causes the changes, what are the implications and what we should do about it. It is about the management and governance of climate change. Risk analysis can have and should have an important role in this management and governance, as risk is a main aspect of climate change: the consequences of climate change are severe and subject to uncertainties. Risk analysis can contribute to improved climate change management and governance by, for example, providing knowledge and guidance on how to:

a) conceptualize and understand climate change risk
b) characterize climate change risk
c) represent and express uncertainties
d) communicate climate change risk
e) understand perceptional aspects related to climate change
f) manage and govern climate change risk
g) understand alternative strategies and policies for handling climate change risk
h) formulate strategies and policies for handling climate change risk

The present book provides such knowledge and guidance. Here is a summary of some key points.

Risk is related to the consequences of an activity, with related uncertainties. The risk is expressed by specifying the consequences and using a measure of uncertainty and adding the knowledge that supports this measure. Climate change is a risk influencing factor, it affects the risk and its characterization.

A company may focus its consequences on economic quantities, and climate change is a factor that can influence these quantities. Using the formalism of Section 4.1, risk can be described by (A,C,U), where A is an event, C its effect and U associated uncertainties. Here, A could be rise in temperature and C an economic quantity. Similar concepts can be defined for a nation or the world. Climate change and related uncertainties are not risk *per se*, unless we relate the consequences directly to the climate change. This is sometimes done, for example when referring to the change in global temperature relative to the 'pre-industrial' levels. The Paris Agreement on climate change aims to ensure increases in global temperature are less than 2°C above 'pre-industrial' levels; hence, a scale of reference can be used to measure the consequences, depending on what will be the actual global temperature. Risk is then defined by the deviation D from 2°C and associated uncertainties. We write Risk = (D,U).

In relation to climate change risk, it is common to refer to physical risk and transition risk, with different types of definitions. Physical risk is risk, as defined above, when we focus on physical changes and impacts, such as sea level rise, floods, droughts and heat waves. It applies to both (A,C,U) and (D,U), with A and D physical quantities. The effects C could be physical but also economic quantities. Transition risk relates to risk associated with the transition to a 'low-carbon society' (less than 2°C above 'pre-industrial' levels). It covers (D,U) types of risk, i.e. risk of not making this transition, as well as risk related to deviations from specified planning scenarios for meeting 2°C, as, for example, given by the Paris Agreement.

From these clarifications, the previous chapters provide knowledge and guidance on how to characterize climate change risk, represent and express uncertainties and communicate climate change risk. Examples are presented, showing that current practice on risk and uncertainty understanding and characterizations suffer from some severe problems and improvements are needed; refer, for example, to Section 6.2.

The literature covers a number of other contributions. For the risk perception insight related to climate change, the present book has addressed some fundamental issues in Section 6.1, to clarify what is risk perception and what are professional judgements of uncertainty and risk. There is a huge body of literature on other aspects linked to risk perception and climate change; see, for example, Visschers (2018).

Chapter 7 provides input to (f), (g) and (h), on management, governance and policies related to climate change risk. As discussed in Chapter 7, when making decisions, the ideal is to be informed by all relevant evidence (including scientific findings) from all relevant stakeholders. Science-based decision-making is often referred to, but it is more accurate to refer to evidence- and knowledge-informed decision-making, as evidence and knowledge can be more or less strong and also erroneous in some cases. The beliefs can be based on assumptions that may turn out to be wrong. Hence, decision-makers also

need to address these limitations and uncertainties related to the knowledge basis. In addition, there could be different values related to the different concerns, which could strongly influence the decision-making. For the climate change issue, there is a strong knowledge base developed, but there are also considerable uncertainties. IPCC summarizes the scientific knowledge base, which includes judgements of uncertainty. Yet, a common perspective is that science has produced a crystal-clear message, which basically prescribes what is now the right thing to do. However, what action is needed is not a scientific question. No recommendations on this matter come from science or risk analysis.

As risk analysts, we are aware that evidence is related to not only facts but also beliefs and concerns that need to be taken into account in risk management and regulation. We are also aware that, as a basis for decision-making, value judgements are equally important, as is evidence in the form of data, information and justified beliefs. Science in general is about balancing 'confidence' (for example, expressing that climate change is mainly man-made) and 'humility' (reflecting that there are uncertainties), and risk analysis is critical for finding this balance and understanding the 'humility' part and seeing the strengths and limitations of the 'confidence' part; refer to the discussion in Sections 3.1.3 and 3.2.3, It is a challenge to find this balance, and one can question whether some of the problems we face today concerning the role of science in society, with 'alternative facts' and lack of authority, can be traced back to the 'humility': this part has not been given the attention it deserves. By strengthening risk analysis, we thus also strengthen other sciences, including climate change research.

In a scientific environment, there is a continuous debate regarding what are the most warranted statements. All beliefs are scrutinized, to see if they can be justified. This is how scientific knowledge is developed over time. The climate change issue is not different, but the political debate and various stakeholders' interests make the discussion challenging. It is often difficult to see what is science and what is politics.

If we choose to give weight to the precautionary and cautionary principles and say that the climate change risk is unacceptable, it is a management and governance policy decision, not a scientific one. We are informed by science and IPCC reports. Through the Paris Agreement, governments all over the world have in fact made such conclusions: actions are needed; the climate change risk is to be reduced. Risk analysis can help in the process of selecting the most effective means, but the actual decisions, as to how quick and in what way this is to be carried out, are outside the scope of risk analysis. Risk analysis supports the decision-making but does not provide the answers.

This chapter is about how to solve practical risk analysis problems. Climate change is a big one. Risk analysis has a role to play, as discussed

above, and the above comments have provided some perspectives on how. It is a discussion that is closely related to the more general debate about science in society and particularly the concept of 'post-normal' science, as introduced by Funtowicz and Ravetz (1993) and mentioned in Section 7.6.3 and the Bibliographic Notes. The present book has a focus on risk and risk analysis, but the fundamental ideas are very much in line with those of the 'post-normal science school'.

8.5 COMPETENCE AND TRAINING IN RISK ANALYSIS

To be able to solve practical risk problems, we need to have human resources (e.g. people, skills, experience), physical and material resources (e.g. computer tools), financial resources (money) and information resources (e.g. databases). The human resources are of special importance: the risk analysis knowledge and competence of people to be able to conduct the risk analysis. This is the topic of the present section.

Section 3.1 and Figure 3.2 illustrate what type of knowledge is needed to conduct risk analysis. There is a fundamental difference between applied risk analysis and generic risk analysis, as discussed in Section 3.1. If we study and govern climate change, risk analysis knowledge is useful to support the assessments and handling, but other types of knowledge – in particular generated by the natural sciences, are really the core ones. For the generic risk analysis, risk analysis knowledge is, however, central, and it defines the field and science of risk analysis.

As discussed in Chapter 3, risk analysis is not broadly recognized as a science *per se* today – there are, for example, few study programmes in risk analysis worldwide. To conduct risk analysis in practice, people from other disciplines have been trained in risk analysis – often limited to a few courses. The implication is that many risk analysts lack proper training in the field and science of risk analysis. In a longer perspective, the result is reduced quality of applied risk analysis. The further development of risk analysis is very much dependent on the degree that we are able to strengthen risk analysis as a field/science and develop good training programmes in risk analysis at our universities and colleges, and elsewhere.

As a field and science, risk analysis has, however, some way to go to obtain broad consensus regarding what represents the core of the discipline. But we are making progress, and the Society for Risk Analysis (SRA) has made an important contribution to this end. An SRA document of core subjects of risk analysis has been developed by a group of experienced and active researchers (SRA 2017a), as discussed in Section 3.1.2. The main

content of the document is included in Appendix B. It covers five main topics: Fundamentals, Risk assessment, Risk perception and communication, Risk management and governance, and Solving real risk problems and issues. All fields (sciences) have some subjects that constitute the core, that all students should cover in basic courses in the field. There will always be a discussion about what this core should be; nonetheless, such a core of subjects is required to obtain the necessary unity and platform for the field and science to develop and be recognized. Risk analysis is no exception. The target audience for the document is all individuals who have an interest in risk analysis, ranging from risk analysis professionals and practitioners to researchers, to students, to decision-makers, to bureaucrats, to regulators, to journalists and to curious laypeople, who would like to obtain an overview of what are the key topics of the field of risk analysis.

A special challenge relates to teaching children and youths about risk and risk analysis. But what should we teach the kids? What are the core subjects to be included in the curriculum? We cannot sell the idea of classes in risk analysis to school administrators and bureaucrats if we do not have a crystal-clear idea of what we wish to obtain, from a short- and a long-term perspective, and what topics should be covered, and how. We need thorough discussions on the matter, as for all fields and sciences. Following ideas by Aven and van Kessenich (2018), we need to highlight an understanding of fundamental concepts – including risk, uncertainty and probability. A second area concerns seeing the difference between professional risk and uncertainty judgements, on the one hand, and risk perceptions, which also reflect aspects like fear, on the other. It is also important to understand that risk is something that is at the same time positive and negative – and we need to find a balance between taking risk (creating values) and reducing risk (protection). And it is essential to see the different perspectives of individuals, organizations and society. From such pillars, we can formulate learning objectives or outcomes, for example that the pupils should be able to discern the difference between professional risk judgements and risk perception. We are seeing the contours of something big here. A lot of work is needed, but we have started. If we can develop risk analysis (risk science) as a school subject, it will certainly be a breakthrough for risk analysis (risk science) in academia and society in general.

9 Perspectives on the future of risk analysis

Today, risk assessment is a well-established tool in situations with considerable data and clearly defined boundaries for its use. Statistical and probabilistic methods have been developed and provide useful decision support for many types of applications. However, risk decisions are, to an increasing extent, about situations characterized by large uncertainties and emergence. Such situations call for different types of approaches and methods, and it is a main challenge for the risk field to develop suitable frameworks and tools for this purpose. The research focus has to highlight dynamic risk assessment and management, rather than static analysis methods.

The concept of emerging risk has gained increasing attention in recent years. Flage and Aven (2015) have performed an in-depth analysis of the emerging risk concept and in particular its relation to black swan type of events through the known/unknown. According to this work, we face emerging risk related to an activity, when the background knowledge is weak but contains indications/justified beliefs that a new type of event (new in the context of that activity) could occur in the future and potentially have severe consequences for something that humans value. The weak background knowledge inter alia results in difficulty specifying consequences and possibly also in fully specifying the event itself; i.e. in difficulty specifying scenarios.

We need to further develop risk analysis that is able to capture these challenges linked to the knowledge dimension and the time dynamics. A pure probabilistic approach, for example a Bayesian analysis, would not be feasible, as the background knowledge – the basis for the probability models and assignments – would be poor. There is a need to balance different risk management strategies in an adaptive manner, including cautionary strategies and attention to signals and warnings.

There is also a need for substantial research and development to obtain adequate modelling and analysis methods – beyond the 'traditional' ones – to 'handle' different types of systems. Examples include critical infrastructures

(e.g. electrical grids, transportation networks, etc.), which are complex systems and often interdependent. Another example is security-type applications, where qualitative assessments are often performed on the basis of judgements of actors' intentions and capacities, without reference to a probability scale. There seems to be a huge potential for significant improvements in the way security is assessed by developing frameworks that integrate the standard security approaches and ways of assessing and treating uncertainty.

Zio (2018) argues that an evolution of risk assessment is in the making, a 'revolution' that takes the form of new approaches to and methods for risk assessment, supported by

- the recognition that the knowledge, information and data (KID) available for analyzing and characterizing hazards, modeling and computing risk are substantially grown and continue to do so;
- the evidence that the modeling capabilities and computational power available have significantly advanced and allow unprecedented analysis with previously infeasible methods;
- the concern that the increased complexity of the systems, nowadays more and more made of heterogeneous elements (hardware, human, digital) organized in highly interconnected structures, leads to behaviors that are diffcult to anticipate or predict, driven by unexpected events and corresponding emerging unknown systems responses;
- the realization that to manage risk in a systematic and effective way it is necessary to consider together all phases of the potential accident scenarios that may occur, including prevention, mitigation, emergency crisis management and restoration, and that this entails an extended vision of risk assessment for an integrated framework of business continuity (with respect to production reliability and availability) and resilience (with respect also to safety);
- the acknowledgment that risk varies significantly over time and so may also the conditions and effectiveness of the prevention, protection and mitigation measures installed;
- the consideration of the need of solid frameworks for the safety and security assessment of cyber-physical systems (CPSs).

(Zio 2018)

Risk assessment is evolving, so are risk understanding, risk characterizations, risk communication, risk management and governance. This is because risk analysis is a science, and there is a continuous development in concepts, principles, theories, approaches, frameworks, methods and models. This is contributed to by the scientific journals, as well as the professional societies and individuals, who have the drive and energy to enhance the risk analysis field and science.

The future of risk analysis, with its components (including assessment, communication, management and policy), has been discussed in many publications; see, for instance, SRA (2015b), Aven and Zio (2014), Venkatasubramanian (2011), Pasman and Reniers (2014) and Khan et al. (2015). The above issues are just examples of the many challenges and opportunities that are addressed. The present book aims at contributing to strengthening the scientific basis of risk analysis and, in this way, to lay down a solid platform for how these challenges and opportunities best can be met. The key idea is that, by building on risk analysis (risk science) as an instrument for generating risk related knowledge, there is huge potential for risk analysis to play an important role in the management and governance of risk-related problems.

Appendix A
Terminology

This appendix summarizes some of the risk analysis and management terminology used in the book. The definitions are in line with the SRA (2015a) Glossary. See this reference for some additional definitions.

The listing is divided into three categories:

I. Terminology of basic concepts
II. Terminology of related concepts, methods, procedures
III. Terminology of risk management actions

The terms are presented in alphabetical order. In the third category, the concept of 'managerial review and judgement' is added. It is not defined in the SRA Glossary. Note that the glossary allows for alternative definitions.

I TERMINOLOGY OF BASIC CONCEPTS

Ambiguity

The condition of admitting more than one meaning/interpretation.

Complex/Complexity

- A system is complex if it is not possible to establish an accurate prediction model of the system based on knowing the specific functions and states of its individual components.
- Complexity: A causal chain with many intervening variables and feedback loops that do not allow the understanding or prediction of the system's behaviour on the basis of each component's behaviour.

Event, Consequences

Event

- the occurrence or change of a particular set of circumstances such as a system failure, an earthquake, an explosion or an outbreak of a pandemic
- a specified change in the state of the world/affairs

Consequences

The effects of the activity, with respect to the values defined (such as human life and health, environment and economic assets), covering the totality of states, events, barriers and outcomes. The consequences are often seen in relation to some reference values (planned values, objectives, etc.), and the focus is often on negative, undesirable consequences.

Exposure

Exposure to something:

- being subject to a risk source/agent (e.g. exposure to asbestos)

Harm, Damage, Adverse consequences, Impacts, Severity

Harm: Physical or psychological injury or damage

Damage: Loss of something desirable

Adverse consequences: Unfavourable consequences

Impacts: The effects that the consequences have on specified values (such as human life and health, environment and economic assets)

Severity: The magnitude of the damage, harm, etc.

Hazard

A risk source where the potential consequences relate to harm. Hazards could, for example, be associated with energy (e.g. explosion, fire), material (toxic or eco-toxic), biota (pathogens) and information (panic communication).

Knowledge

Two types of knowledge:

Know-how (skill) and know-that of propositional knowledge (justified beliefs).

Knowledge is gained through, for example, scientific methodology and peer-review, experience and testing.

Model

A model of an object (e.g. activity, system) is a simplified representation of this object.

A probability model is a special type of model, based on frequentist probabilities (often referred to as chances in a Bayesian context).

Opportunity

An element (action, sub-activity, component, system, event, . . .), which alone or in combination with other elements has the potential to give rise to some specified desirable consequences

Probability

Either a knowledge-based (subjective) measure of uncertainty of an event, conditional on the background knowledge or a frequentist probability (chance). If a knowledge-based probability is equal to 0.10, it means that the uncertainty (degree of belief) is the same as randomly drawing a specific ball out of an urn. A frequentist probability (chance) is the fraction of events A occurring when the situation under consideration can be repeated over and over again infinitely. See the SRA Glossary (2015a) and Section 4.2 for further details.

Resilience

Overall qualitative definitions

Resilience is the ability of the system to sustain or restore its basic functionality following a risk source or an event (even unknown).

Resilience metrics/descriptions (examples)

– The probability that the system is able to sustain operation when exposed to some types of risk sources or events (which can be more or less accurately defined)

A resilient system is a system for which the resilience is judged to be high (this is a value judgement).

Risk

See Chapter 4. In its most general form:

Risk is the two-dimensional combination of the consequences C of the activity (with respect to something that humans value) and associated uncertainties about C.

Risk description: A qualitative and/or quantitative picture of the risk, i.e. a structured statement of risk usually containing the elements: risk sources, causes, events, consequences and uncertainty representations/measurements. Formally we write:

Risk description = (C',Q,K),

where C' is the specified consequences of the activity considered, Q the measure of uncertainty used, and K the background knowledge that C' and Q are based on.

Risk source or risk agent

An element (action, sub-activity, component, system, event, . . .), which alone or in combination with other elements has the potential to give rise to some specified consequences (typically undesirable consequences).

Robustness

The antonym of vulnerability

Safe, safety

Safe

Without unacceptable risk

Safety

- Interpreted in the same way as safe (e.g. when saying that safety is achieved)
- The antonym of risk (the safety level is linked to the risk level; a high safety level means a low risk level and vice versa)

Sometimes limited to risk related to non-intentional events (including accidents and continuous exposures)

Security, secure

Secure

Without unacceptable risk when restricting the concept of risk to intentional acts by intelligent actors

Security

- Interpreted in the same way as secure (e.g. when saying that security is achieved)
- The antonym of risk when restricting the concept of risk to intentional acts by intelligent actors (the security level is linked to the risk level; a high security level means a low risk level and vice versa)

Threat

Risk source, commonly used in relation to security applications (but also in relation to other applications, e.g. the threat of an earthquake)

Threat in relation to an attack: A stated or inferred intention to initiate an attack with the intention to inflict harm, fear, pain or misery

Uncertainty

Overall qualitative definitions

- For a person or a group of persons, not knowing the true value of a quantity or the future consequences of an activity
- Imperfect or incomplete information/knowledge about a hypothesis, a quantity, or the occurrence of an event

Uncertainty metrics/descriptions (examples)

- A subjective probability
- The pair *(Q,K)*, where Q is a measure of uncertainty and K the background knowledge that supports Q

Epistemic uncertainty

As above for the overall qualitative definition of uncertainty and uncertainty metrics/descriptions (examples)

Aleatory (stochastic) uncertainty

Variation of quantities in a population of units (commonly represented/described by a probability model)

Vulnerability

Overall qualitative definitions

- The degree a system is affected by a risk source or agent
- The degree a system is able to withstand specific loads
- Vulnerability is risk conditional on the occurrence of a risk source/agent

Vulnerability metrics/descriptions (examples)

As for risk, but conditional on the risk source or event (load)

- Expected loss given a failure of a single component or multiple components
- Expected number of fatalities given the occurrence of a specific event
- Expected system loss under conditions of stress
- The probability that the system capacity is not able to withstand a specific load (the capacity is less than the load)
- A probability distribution for the loss given the occurrence of a risk source
- (C', Q, K | risk source) (i.e. a risk description given the occurrence of a risk source; see Section 4.2)

As for risk, the suitability of these metrics/descriptions depends on the situation.

A vulnerable system is a system whose level of vulnerability is judged to be high.

II TERMINOLOGY OF RELATED CONCEPTS, METHODS, PROCEDURES

Model uncertainty

Uncertainty about the model error, i.e. about the difference between the model output and the true value being modelled

Precautionary principle

An ethical principle expressing that if the consequences of an activity could be serious and subject to scientific uncertainties, then precautionary measures should be taken, or the activity should not be carried out

Risk analysis

Systematic process to comprehend the nature of risk and to express the risk, with the available knowledge

Risk analysis is often also understood in a broader way, in particular in the Society for Risk Analysis (SRA) community: risk analysis is defined to include risk assessment, risk characterization, risk communication, risk management, and policy relating to risk, in the context of risks of concern to individuals, to public and private sector organizations, and to society at a local, regional, national, or global level.

Risk appetite

Amount and type of risk an organization is willing to take on risky activities in pursuit of values or interests

Risk assessment

Systematic process to comprehend the nature of risk, express and evaluate risk, with the available knowledge

Risk aversion

Disliking or avoiding risk

Technical definition: Risk aversion means that the decision-maker's certainty equivalent is less than the expected value, where the certainty equivalent is the amount of payoff (e.g. money or utility) that the decision-maker has to receive to be indifferent between the payoff and the actual "gamble".

Risk characterization, risk description

A qualitative and/or quantitative picture of the risk, i.e. a structured statement of risk usually containing the elements: risk sources, causes, events, consequences, uncertainty representations/measurements (e.g. probability distributions for different categories of consequences – casualties, environmental damage, economic loss, etc.) and the knowledge that the judgements are based on. See also the definition of risk description in relation to the definition of the concept of 'risk'.

Risk communication

Exchange or sharing of risk-related data, information and knowledge between and among different target groups (such as regulators, stakeholders, consumers, media, general public)

Risk evaluation

Process of comparing the result of risk analysis (see 'Risk analysis') against risk (and often benefit) criteria to determine the significance and acceptability of the risk

Risk framing (pre-assessment)

The initial assessment of a risk problem, clarifying the issues and defining the scope of subsequent work

Risk governance

Risk governance is the application of governance principles to the identification, assessment, management and communication of risk. Governance refers to the actions, processes, traditions and institutions by which authority is exercised and decisions are taken and implemented.

Risk governance includes the totality of actors, rules, conventions, processes and mechanisms concerned with how relevant risk information is collected, analysed and communicated and management decisions are taken.

Risk management

Activities to handle risk such as prevention, mitigation, adaptation or sharing

It often includes trade-offs between costs and benefits of risk reduction and choice of a level of tolerable risk.

Risk perception

A person's subjective judgement or appraisal of risk

III TERMINOLOGY OF RISK MANAGEMENT ACTIONS

Managerial review and judgement

Process of summarizing, interpreting and deliberating over the results of risk assessments and other assessments, as well as of other relevant issues (not covered by the assessments), in order to make a decision

This definition is not given in the SRA Glossary.

Risk acceptance

An attitude expressing that the risk is judged acceptable by a particular individual or group

Risk policy

A plan for action on how to manage risk

Risk prevention

Process of actions to avoid a risk source or to intercept the risk source pathway to the realization of damage, with the effect that none of the targets is affected by the risk source

Risk reduction

Process of actions to reduce risk

Risk regulation

Governmental interventions aimed at the protection and management of values subject to risk

Risk sharing or pooling

Form of risk treatment involving the agreed distribution of risk among other parties

Risk tolerance

An attitude expressing that the risk is judged tolerable

Risk trade-offs (risk-risk trade-offs)

The phenomenon that intervention aimed at reducing one risk can increase other risks or shift risk to another population or target

Risk transfer

Sharing with another party the benefit of gain, or burden of loss, from the risk
Passing a risk to another party

Risk treatment

Process of actions to modify risk

Stakeholder involvement (in risk governance)

The process by which organizations or groups of people who may be affected by a risk-related decision can influence the decisions or their implementation

Appendix B

Subjects and topics defining the risk analysis field

In a recent document from the Society for Risk Analysis, a list of the core subjects of risk analysis is presented (SRA 2017a). It captures five main categories of subjects: fundamentals (science, knowledge, uncertainties, risk – other basic concepts); risk assessment; risk perception and communication; risk management and governance; and solving real risk problems and issues.

The objectives of the document are:

1. "To initiate and foster a discussion on what are the core subjects of risk analysis.
2. To provide guidance on what subjects should be covered in study programs on risk analysis, for example a two-year Master program.
3. To offer a platform on which to identify key topics for study programs on specific risk analysis subjects like risk assessment or risk management, for broad overview courses on risk analysis, as well as for courses and programs on related areas such as safety and security.

In more general terms, the document gives a contribution to the overall goal of establishing the knowledge content pillars for risk analysis as a science in itself." (SRA 2017a).

"1 FUNDAMENTALS

This area covers fundamental issues related to risk analysis as a field and science, basic concepts and principles, including ways of representing and expressing uncertainties. The SRA Glossary represents a possible basis for this category of subjects.

More specific topics:
What is risk analysis? Different analysis approaches used and issues raised [such as a–h listed in Section 3.1.1]. The risk analysis field and science. The distinction between A and B type of risk analysis knowledge generation (applied risk analysis and generic risk analysis, see Section 3.1). The risk concept (basic ideas, alternative definitions with discussion). Risk metrics. Coherent risk metrics. Risk and knowledge. Surprises and the unforeseen (black swans). Risk and utility. Risk aversion. Why risk is not expected value or variance. Representing and expressing uncertainties. Different types of uncertainties (epistemic, aleatory). The probability (likelihood) concept. Variation and probability models. Frequencies. Understanding and using subjective probabilities to reflect epistemic uncertainties and degrees of belief. Why the use of probability to represent uncertainties? Bayesian analysis. Generalizations of probability theory. Interval (imprecise) probabilities and related 'non-probabilistic' characterizations and metrics. Risk problem categorizations (e.g. simple, complex, uncertain, ambiguous). Fundamentals about modelling of systems and processes in a risk context. Different types of models (structural models, physical models, logic models, probability models). Model uncertainty. Causality, uncertainties and risk. Sensitivity analysis and importance measures analysis.

Related concepts like hazards, threats, opportunities, danger, vulnerabilities, resilience, safety, security, risk source, reliability, etc.; commonalities and distinctions.

2 RISK ASSESSMENT

This area covers principles, approaches, and methods for identifying risk sources, threats, hazards and opportunities; understanding how these can occur and what can be their consequences including adaptive behaviour and recovery; representing and expressing uncertainties and risk; and determining the significance of the risk using relevant criteria.

More specific topics:
Stages and processes in a risk assessment: planning, identification, cause analysis, consequence analysis, uncertainties and beliefs, evaluation. Main categories of assessment approaches, including statistical approaches and system analytical approaches; qualitative, quantitative and semi-quantitative; dynamic and semi-dynamic/static; linear and non-linear approaches. Models for analysing failures, events, survival, causation, frequency-severity, interactions, etc. Dose-response functions. Meta analyses. Methods for addressing potential surprises and the unforeseen. Reflecting signals and warnings. Adaptive risk assessments. Quality of risk assessment (validity, reliability criteria).

Specific approaches, methods and models

Risk source identification and qualitative analysis methods such as databases, brainstorming, Delphi methods, interviews, surveys, checklists, Structured What IF Technique (SWIFT), HAZard Operability studies (HAZOP), Anticipatory Failure Determination (AFD), red teaming, etc. Basic analysis tools such as block diagrams, fault trees, event trees, Bayesian belief networks, Bow-tie diagrams and Monte Carlo simulation. Advanced analysis tools like complex network theory, agent-based modelling, etc. Expert judgements, including heuristics and biases. Deriving and using different types of models such as counting processes (e.g. Poisson), marked point processes (e.g. Compound Poisson process), survival models (e.g. Weibull), times series models, artificial intelligence models, causal models, logistic regression models, game theory models, etc. Related statistical analysis (including Bayesian).

Design of the analysis

Characterization of the problem and associated analysis tasks. Evaluation of strength and weaknesses of assessment approaches and methods. Choosing the proper approaches and methods for assessing the risk, including approaches and methods for representing and treating interdependencies, uncertainties and knowledge. Protocol for dealing with complexity, uncertainty and ambiguity, as well as potential surprises and the unforeseen.

Evaluation

Presentations of the results of the risk assessments, with characterization of knowledge, uncertainties and limitations. Decision criteria. Tolerability limits and acceptance criteria. Risk-risk comparisons. Differences in risk perspectives between analysts and decision-makers. Decision frameworks; integration with other types of analyses, such as social impact analyses, technology assessments, and cost-benefit analysis. Risk valuation.

3 RISK PERCEPTION AND COMMUNICATION

This area covers issues related to perception and communication of risk, how affect and trust influence risk perception and behaviour, and how exchange or sharing of risk-related data, information and knowledge between and among different parties (such as regulators, experts, consumers, media, general public) can be provided.

More specific topics:
What is risk perception? Risk perception and feelings/affects. Reactions to real or perceived threats: System 1 vs. System 2. What are the determinants

of perceived risk? The difference between expert versus lay judgements of risk. How and why do laypersons' perceptions of risk differ from those of the experts? Heuristics, biases, beliefs and risk perception. Social and cultural factors shaping risk perception. How social trust and credibility relate to risk perception. Risk perception and behaviour/decisions. The psychometric model. The cultural theory of risk perception. Social amplification of risk.

What is risk communication? Different models and theories of communication related to risk. Risk information seeking and processing. Sources of risk information, including unofficial. Message design and the effects of different message elements, such as probabilities, comparisons, statistics, narratives, fear appeals. Media coverage of risk. Different types of stakeholders and audiences. Strategic risk communication. Visuals in risk communication. Framing effects on risk perceptions and behaviours. Persuasive and balanced messages. Source credibility and its influence on message effects. Public engagement to inform risk analysis. The analysis-deliberation paradigm.

4 RISK MANAGEMENT AND GOVERNANCE

This area covers measures and activities carried out to manage and govern risk, balancing developments and exploring opportunities, on the one hand, and avoiding losses, accidents and disasters on the other. A main emphasis here is on providing insights and guidance on multi-dimensional, multi-actor, multi-institutional decision- and policy-making and on resolving emerging trade-offs.

More specific topics:
Risk management strategies and processes. Risk avoidance, optimization, reduction, transfer, sharing, retention, acceptance and tolerability. What risky prospects to accept? How to allocate resources across risky opportunities? Different types of risk problems. Decision mistakes and how to avoid them. Preferences, goal setting and performance measures. Risk trade-offs. Enterprise risk management. Insurance.

Different instruments and tools. Multi-criteria, multi-attribute, multi-actor types of analyses. Cost-benefit analysis. Value of a Statistical Life (VSL). Bayesian decision analysis. Expected utility theory. Alternatives to expected utility theory (including Prospect theory).

Cooperative risk management. Principal-Agent (P-A) model of risk management. Negotiation and bargaining. Games. Adversarial risk analysis. Risk psychology for groups, organizations, crowds, and markets. Group-thinking and dynamics. Consensus. Building a risk culture. High reliability organizations (HRO).

Cautionary and precautionary principles. Robustness and resilience-based approaches. ALARP (As Low As Reasonably Practicable).

Adaptive risk management. Black swans. Emergency preparedness planning. Disaster planning. Policy analysis and risk. Risk governance issues (e.g. regulatory styles, regulatory regimes, risk governance capacity building, risk governance performance). The analysis-deliberation paradigm.

Modes of collective decision-making. How to reach consensus on difficult conflicting values and trade-offs? Stakeholder involvement. Public participation. Law and risk management (the legal context). Risk regulation. Standards, inspection and certification. Risk analysis and politics. Ethical aspects.

5 SOLVING RISK PROBLEMS AND ISSUES

This category of subjects addresses how to solve risk problems, challenges and issues in real practice, by integrating theories and methods from the other four categories of topics, and using concrete, practical cases. Risk analysis as a multidisciplinary and interdisciplinary field is demonstrated, and special attention is devoted to the added value of risk analysis relative to the contributions from other fields and sciences. Organizational capacity (human resources, knowledge, etc.) needed for achieving high quality risk analysis is a key topic.

Cases are considered, highlighting

i. Clarification of the problem, challenge or issue, such as (see also a)-h) in Section 3.1.1):
   a. Support decision-making on choice of alternatives and measures
   b. "Prove" that an activity is safe
   c. Empower people with risk related knowledge
   d. Reduce concerns and increase trust and confidence

ii. Approaches for knowledge generation and management
   a. Frameworks and processes (including standards)
   b. Methods and tools

iii. Execution and results obtained. Challenges and reflections, covering issues like
   - The degree to which the risk assessment is engaged effectively in the risk management decision process
   - The risk characterization has a format suitable for the decision-making situation
   - The degree to which disclosure of the actual role of the analysis, e.g. advise vs defend, is practised
   - The degree to which assumptions and caveats, and the implications of these for the decision-making, has been stated
   - Potential surprises are addressed, and relevant management strategies implemented

iv. Institutional responses to risk challenges. Role of risk regulation. Capacity building for risk assessment, management and governance; dealing with transboundary risks, international cooperation and legal requirements

Examples of cases that could be included:

- Accident risk analysis of engineering systems such as nuclear power plants, offshore installations, aircrafts and spaceships, critical infrastructures. First, second, and third party risks. How safe is safe enough? Probabilistic risk assessment (PRA). Quantitative Risk Assessment (QRA).
- Consumer product safety. Perceived vs. historical data. Examples: Plastic baby bottles. Silicon breast implants, seatbelts, etc.
- Food and drug safety. Contaminants (deliberate or accidental) in foods and drinks. Microbial safety and microbial risk assessment. How sure can we be? GMO safety. BSE
- Occupational safety. Framework: Asymmetries in information and costs of care. How much care should employers and employees be required to take? Hazardous occupations. Industrial hygiene.
- Transportation safety. Maritime safety, aviation safety, railroad safety, automobile safety.
- Public health risk assessments. Epidemics, pandemics. Exposure modelling and analysis. False positives. Risk management policy paradigms: Command/control; nudge: information and incentives; and adapt: experiment, learn, and share successes.
- Environmental and ecological risk analysis. Climate change. Acid rain. Conserving biodiversity. Sustainable management of natural resources
- Financial risk analysis. Credit risk analysis. Investment risk analysis. Financial portfolio risk analysis. Financial market risks. Corporate financial risk management. Personal financial risk management.
- Security and terrorism. Cyberterrorism and cyber-security risk. Alternative analysis frameworks. Risk and uncertainty conceptualization and characterization.
- Habitual risk. Smoking, different lifestyles, cultural practices.
- Social risks: lack of social coherence, growing inequities, crime, war, civil war, violence." (SRA 2017a)

Bibliographic notes

Chapter 1 of this book is based on Aven (2011c, 2015c, 2018b, 2019c, e) and Aven and Renn (2015, 2019). For other publications providing illustrating examples of the importance of risk analysis and risk science, the reader is referred to Meyer and Reniers (2013), Greenberg (2017) and Cox et al. (2018).

The main sources for Chapter 2 on the fundamentals of science, knowledge and research are Hansson and Aven (2014) and Aven (2014a, 2019a). Chapter 3 on the foundation of the risk science is, to a large extent, based on Hansson and Aven (2014), Aven (2014a, 2017a, 2018a, 2019a) and SRA (2015a, 2017a, b). There is a vast body of literature on science and scientific perspectives which relates to risk. Amongst the most relevant for the present discussion is the concept of 'post-normal' science, as introduced by Funtowicz and Ravetz (1990, 1993); see also Ravetz and Funtowicz (1999), Funtowicz and Strand (2007) and Saltelli and Funtowicz (2017), refer to Section 7.6.3. By classifying problem-solving strategies into a model for applied sciences, professional consultancy and post-normal sciences, these authors provide a framework for discussing issues related to quality in scientific work, as well as managerial and political implications. As commented by Aven (2013a), the ideas of Funtowicz and Ravetz can be placed in a general scientific risk framework based on the risk perspectives used in this book. The model of Funtowicz and Ravetz comprises the two axes: i) decision stakes – the value dimension (costs, benefits) and ii) system uncertainties – the knowledge dimension. These axes resemble the same two dimensions that characterize risk as used in this book; see Section 4.1.

Chapter 4, on the risk concept and its description, is based on SRA (2015a), Aven (2012a, 2017c, 2019a) and Amundrud and Aven (2015). The idea of seeing risk as capturing the two dimensions, consequences and uncertainties, goes back to the 1980s if not further. In their celebrated

paper, Kaplan and Garrick (1981) refer to risk as qualitatively defined as "uncertainties + damage", which can be viewed as a (C,U) type of definition. However, these scholars did not develop a theory as presented in this book and as in, for example, Aven (2014b). This theory, which captures the '(C,U) – (C'Q,K)' logic, is built on early work by Aven (2000) and Aven and Kristensen (2005). For a discussion of the ontological status of the concept of risk, see Rosa (1998), Aven et al. (2011) and Solberg and Njå (2012). The concept of surprises (black swans) is thoroughly discussed in Aven (2014b). See Gross (2010, p. 39) and NOG (2017) for some industrial examples of surprises. For further discussion of the differences in different perspectives on how to describe uncertainties in risk assessments, see Aven et al. (2014), Flage et al. (2014, 2018).

Taleb (2007) made the black swan metaphor well-known, and it is widely used today. His work has inspired many authors, also on foundational issues (e.g. Chichilnisky 2013, Feduzi and Runde 2014, Masys 2012, Aven 2014b, 2015a), and recently there has been a lively discussion about the meaning of the black swan metaphor and its use in risk management; see Haugen and Vinnem (2015) and Aven (2015d, e). The metaphor has created a huge interest in risk, particularly among laypersons. It has also created increased focus, in the professional risk analysis society, on risk, knowledge and surprises. Different types of black swans have been defined and measures to meet them discussed (e.g. Paté-Cornell 2012, Aven and Krohn 2014, Aven 2015d). But it is just a metaphor and cannot replace the need for conceptual precision linked to terms such as 'risk', 'probability' and 'knowledge'. As highlighted by Aven (2015b), the basic idea of addressing black swans is to obtain a stronger focus on issues not covered by the traditional risk perspectives, highlighting historical data, probabilities and expected values (the world of Mediocristan in Taleb's terminology). Surprises do occur relative to the beliefs determined by these measures and concepts (historical data, probabilities and expected values). We need to have greater focus on the world outside Mediocristan, what Taleb refers to as Extremistan. Approaches to meet the potential surprises and black swans include improved risk assessments, better capturing the knowledge dimension (refer Section 4.2 and Chapter 7), and adaptive and resilient thinking and analysis, as discussed in the references mentioned at the beginning of this paragraph. The importance of assumptions in risk assessments context have been addressed by many authors, including Beard (2004), Paté-Cornell (1996), Berner and Flage (2016a, 2017) and Khorsandi and Aven (2017).

Chapter 5 is built on Aven (2016b, c, d, e), Aven and Zio (2013) and Bjerga et al. (2014, 2018). Section 5.1, which addresses the concepts of reliability and validity, is based on Aven and Heide (2009) but extends the analysis to update it on the current risk knowledge. The work by Paté-Cornell (1996)

addresses several of the issues discussed by Aven (2016d) and presented in Section 5.2. The concept of model uncertainty is pivotal in risk assessment and has been studied by several authors (see e.g. Zio and Apostolakis (1996), Devooght (1998), Nilsen and Aven (2003), Helton et al (2004), Rosqvist and Tuominen (2004a, 2004b), Droguett and Mosleh (2008, 2014) and Aven and Zio (2013)), but there remains a lack of consensus on how to treat it in practice and even on the meaning to be given to it. It comes naturally to address model uncertainty when there are alternative plausible hypotheses for modelling the specific phenomena or events of interest (Parry and Drouin 2009, Reinert and Apostolakis 2006), but it can also be evoked in relation to the difference between the actual values of the real-world output and the values predicted by the model (Östergaard et al. 1996, Kaminski et al. 2008, Nilsen and Aven 2003). Droguett and Mosleh (2008) also talk about model uncertainty in situations where a single model is generally accepted but not completely validated, a conceptually accepted and validated model is of uncertain quality of implementation, a single model covers only some and not all relevant aspects of the problem, and when composite models are formed by submodels of differing degrees of accuracy and credibility.

The discussion about rare events in Section 5.4 is closely related to the concepts of common causes and special causes referred to in the quality discourse (Shewhart 1931, 1939, Deming 2000, Bergman 2009). These two concepts refer, respectively, to variation that is predictable in the view of the historical experience base and to variation that is unpredictable and outside the historical experience base (it always comes as a surprise). For further discussion on rare events and surprises, see Section 7.3, Paté-Cornell (2012) and Aven (2014b). A basic reference is also Weich and Sutcliffe (2007), linking surprises with resilience and the concept of organizational mindfulness. The topic of surprise and the unforeseen is not discussed in detail in Kaplan and Garrick (1981) but these authors make some interesting points related to the issue when arguing for including scenario categories of the type 'others' to ensure completeness and reflect potential surprises. It is another example showing these authors' groundbreaking ideas and work, which have strongly influenced the risk field and science (Aven 2019a).

As for all the main areas of risk analysis, there is a vast literature available on risk perception and communication. Chapter 6 refers to some key publications, including Tversky and Kahneman (1974), Slovic (1987), Pidgeon (1998) Rohrmann and Renn (2000) and Renn (1998b, 2008). The main contribution of the chapter is based on Aven (2015c, 2018b, d) and Veland and Aven (2013). These papers relate the perception and communication of risk to risk understanding and the risk science.

Chapter 7 provides a discussion of selected fundamental topics within risk management and governance. The chapter is, to a large extent, based

on Aven (2016a, 2017b, 2019a, b, c), Aven and Renn (2018, 2019) and SRA (2015b). For basic literature on risk management and governance, see Fischhoff et al. (1981), Paté (1983), Hood et al. (2001), Kirwan et al. (2002), Renn (2008), Hopkin (2010), Aven and Renn (2010), Meyer and Reniers (2013), Rosa et al. (2014) and Greenberg et al. (2015). For some reflections on how risk regulation is affected by the risk perspectives studied in this book, see Aven and Ylonen (2016). A basic reference for the use of managerial review and judgements in risk analysis is Hertz and and Thomas (1983).

The book emphasizes that risk assessment supports decision-making but does not prescribe what is the best decision. There are other concerns than risk that need to be taken into account when making decisions in situations where risk is an issue. Some type of decision analysis is in place. A backbone in decision analysis is the expected subjective utility theory. It is discussed in a number of papers in risk analysis including Paté-Cornell (1996). The theoretical basis and its usefulness for guiding risk decisions are acknowledged, but also its limitations. Paté-Cornell provides a thorough discussion of the topic. She points to the fact that a rational decision maker according to the expected utility theory is assumed to be indifferent to the level of uncertainty (ambiguity) beyond its effect on the outcome subjective probability distribution. Whether the probability is founded on a strong or weak knowledge basis is not relevant. She refers to 'firm' and 'soft' probabilities, respectively. However, ignoring this aspect of knowledge strength can be challenged from both an empirical and normative perspective as discussed by Paté-Cornell, and followed up by a number of researchers in recent years (see e.g. Gilboa and Marinacci 2013 and Aven 2012d, pp. 120–2). Paté-Cornell has made an important contribution on this issue, by clarifying the difference between risk analysis and decision analysis. Her analysis is to large extent also state-of-the-art of today (Aven 2019a).

Chapter 8 is based on Aven (2017e, 2018b, c), Aven and Ylonen (2019), Bjerga and Aven (2016) and Aven and Michiels van Kessenich (2019). Chapter 9 is partly based on Aven (2016a).

References

Abrahamsen, E. and Aven, T. (2012) Why risk acceptance criteria need to be defined by the authorities and not the industry. *Reliability Engineering System Safety*. 105, 47–50.

Ackoff, R.L. (1989) From data to wisdom. *Journal of Applied Systems Analysis*, 16, 3–9.

Aldred, J. (2013) Justifying precautionary policies: Incommensurability and uncertainty. *Ecological Economics*, 96, 132–40.

Ale, B.J.M. (2002) Risk assessment practices in the Netherlands. *Safety Science*, 40, 105–26.

Ale, B.J.M., Hartford, D.N.D. and Slater, D. (2015) ALARP and CBA all in the same game. *Safety Science*, 76, 90–100.

Ale, B.J.M., Hartford, D.N.D. and Slater, D. (2018) The practical value of life: Priceless or a CBA calculation? *Medical Research Archives*, 6(3), 1–12.

Althaus, C.E. (2005) A disciplinary perspective on the epistemological status of risk. *Risk Analysis*, 25(3), 567–88.

Althaus, C., Bridgman, P. and Davis, G. (2018) *The Australian Policy Handbook*. 6th ed. Crows Nest, New South Wales: Allen & Unwin.

Amundrud, Ø. and Aven, T. (2015) On to understand and acknowledge risk. *Reliability Engineering and System Safety*, 142, 42–7. Open Access.

Amundrud, Ø., Aven, T. and Flage, R. (2017) How the definition of security risk can be made compatible with safety definitions. In Proceedings of the Institution of Mechanical Engineers, Part O: *Journal of Risk and Reliability*, 231(3), 286–94, Open Access.

Apostolakis, G.E. (2004) How useful is quantitative risk assessment? *Risk Analysis*, 24(3), 515–20.

Arnould, J. and Grabowski, H. (1981) Auto safety regulation: An analysis of market failure. *The Bell Journal of Economics*, 12 (1), 27–48.

Askeland, T., Flage, R. and Aven, T. (2017) Moving beyond probabilities – strength of knowledge characterisations applied to security. *Reliability Engineering and System Safety*, 159, 196–205.

Aven, E. and Aven, T. (2015) On the need for rethinking current practice which highlights goal achievement risk in an enterprise context. *Risk Analysis*, 35(9), 1706–16.

Aven, T. (2000) Risk analysis – a tool for expressing and communicating uncertainty. In M.P. Cottam, D.W. Harvey, R.P. Pape and J. Tait (eds), *Proceedings ESREL 2000, Edinburgh 15–17 May 2000*. Rotterdam: Balkema Publishers, 21–8.

Aven, T. (2010a) Some reflections on uncertainty analysis and management. *Reliability Engineering and System Safety*, 95, 195–201.

Aven, T. (2010b) On the need for restricting the probabilistic analysis in risk assessments to variability. *Risk Analysis*, 30(3), 354–60. With discussion 381–4.

Aven, T. (2010c) *Misconceptions of Risk*. Chichester: Wiley.

Aven, T. (2011a) On different types of uncertainties in the context of the precautionary principle. *Risk Analysis*, 31(10), 1515–25. With discussion 1538–42.

Aven, T. (2011b) *Quantitative Risk Assessment. The Scientific Platform*. Cambridge: Cambridge University Press.

Aven, T. (2011c) Selective critique of risk assessments with recommendations for improving methodology and practice. *Reliability Engineering and System Safety*, 96, 509–14.

Aven, T. (2012a) The risk concept. Historical and recent development trends. *Reliability Engineering and System Safety*, 115, 136–45.

Aven, T. (2012b) On the link between risk and exposure. *Reliability Engineering and System Safety*, 106, 191–9.

Aven, T. (2012c) On when to base event trees and fault trees on probability models and frequentist probabilities in quantitative risk assessments. *International Journal of Performability Engineering*, 8(3), 311–20.

Aven, T. (2012d) Foundational issues in risk assessment and management. *Risk Analysis*, 32(10), 1647–56.

Aven, T. (2013a) On Funtowicz & Ravetz's "decision stake – system uncertainties" structure and recently developed risk perspectives frameworks. *Risk Analysis*, 22(2), 270–80.

Aven, T. (2013b) On how to deal with deep uncertainties in a risk assessment and management context. *Risk Analysis*, 33(12), 2082–91.

Aven, T. (2013c) Probabilities and background knowledge as a tool to reflect uncertainties in relation to intentional acts. *Reliability Engineering and System Safety*, 119, 229–34.

Aven, T. (2013d) A conceptual framework for linking risk and the elements of the data-information-knowledge-wisdom (DIKW) hierarchy. *Reliability Engineering and System Safety*, 111, 30–6.

Aven, T. (2013e) Practical implications of the new risk perspectives. *Reliability Engineering and System Safety*, 115, 136–45.

Aven, T. (2014a) What is safety science? *Safety Science*, 67, 15–20.

Aven, T. (2014b) *Risk, Surprises and Black Swans*. New York: Routledge.

Aven, T. (2015a) The concept of antifragility and its implications for the practice of risk analysis. *Risk Analysis*, 35(3), 476–83.

Aven, T. (2015b) Implications of black swans to the foundations and practice of risk assessment and management. *Reliability Engineering and System Safety*. 134, 83–91. Open Access.

Aven, T. (2015c) On the allegations that small risks are treated out of proportion to their importance. *Reliability Engineering and System Safety*, 140, 116–21. Open Access.

Aven, T. (2015d) Comments to the short communication by Jan Erik Vinnem and Stein Haugen titled "Perspectives on risk and the unforeseen". *Reliability Engineering and System Safety*, 137, 69–75.
Aven, T. (2015e) *Risk Analysis*. 2nd ed. Chichester: Wiley.
Aven, T. (2016a) Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 25, 1–13. Open Access.
Aven, T. (2016b) Ignoring scenarios in risk assessments: Understanding the issue and improving current practice. *Reliability Engineering and System Safety*, 145, 215–20.
Aven, T. (2016c) On the difference between risk as seen from the perspectives of the analysts and management. *ASME Journal, Risk uncertainty* Part B 2(3), 031002 1–7.
Aven, T. (2016d) On conservatism in risk assessments. *Reliability Engineering and System Safety*, 146, 33–8.
Aven, T. (2016e) Supplementing quantitative risk assessments with a stage addressing the risk understanding of the decision maker. *Reliability Engineering and System Safety*, 152, 51–7.
Aven, T. (2017a) What defines us as professionals in the field of risk analysis? *Risk Analysis*, 37(5), 854–60.
Aven, T. (2017b) On some foundational issues related to cost-benefit and risk. *International Journal of Business Continuity and Risk Management*, 7(3), 182–91.
Aven, T. (2017c) Improving risk characterisations in practical situations by highlighting knowledge aspects, with applications to risk matrices. *Reliability Engineering and System Safety*, 167, 42–8.
Aven, T. (2017d) How some types of risk assessments can support resilience analysis and management. *Reliability Engineering and System Safety*, 167, 536–43.
Aven, T. (2017e) The flaws of the ISO 31000 conceptualisation of risk. *Journal of Risk and Reliability*, editorial, 231(5), 467–8.
Aven, T. (2018a) An emerging new risk analysis science: Foundations and implications. *Risk Analysis*, 38(5), 876–88.
Aven, T. (2018b) Perspectives on the nexus between good risk communication and high scientific risk analysis quality. *Reliability Engineering and System Safety*, 178, 290–6.
Aven, T. (2018c) Further reflections on EFSA's work on uncertainty in scientific assessments. *Journal of Risk Research*. DOI: 10.1080/13669877.2017.1391321.
Aven, T. (2018d) How the integration of System 1-System 2 thinking and recent risk perspectives can improve risk assessment and management. *Reliability Engineering and System Safety*, 20, 237–44.
Aven, T. (2018e) The meaning of a black swan. In V. Bier (ed.), *Risk in Extreme Environments*. New York: Routledge.
Aven, T. (2018f) Reflections on the use of conceptual research in risk analysis. *Risk Analysis*, 38(11), 2415–23.
Aven, T. (2019a) Three influential risk foundation papers from the 80s and 90s: Are they still state-of-the-art?
Aven, T. (2019b) The call for a shift from risk to resilience: What does it mean? *Risk Analysis*.
Aven, T. (2019c) The cautionary principle in risk management: Foundation and practical use.

Aven, T. (2019d) How to determine the largest global and national risks: Review and discussion.
Aven, T. (2019e) The neglected pillar of science: Risk and uncertainty analysis.
Aven, T., Baraldi, P., Flage, R. and Zio, E. (2014) *Uncertainty in Risk Assessment*. Chichester: Wiley.
Aven, T. and Bergman, B. (2012) A conceptualistic pragmatism in a risk assessment context. *International Journal of Performability Engineering IJPE*, 8(3), 223–32.
Aven, T. and Cox, T. (2016) National and global risk studies: How can the field of risk analysis contribute? *Risk Analysis*, 36(2), 186–90.
Aven, T. and Flage, R. (2018) Risk assessment with broad uncertainty and knowledge characterisations: An illustrating case study. In T. Aven and E. Zio (eds), *Knowledge in Risk Assessments*, 3–26. New York: Wiley.
Aven, T. and Heide, B. (2009) Reliability and validity of risk analysis. *Reliability Engineering and System Safety*, 94, 1862–8.
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. (2019) How the distinction between general knowledge and specific knowledge can improve the foundation and practice of risk assessment and risk-informed decision-making.
Aven, T. and Krohn, B.S. (2014) A new perspective on how to understand, assess and manage risk and the unforeseen. *Reliability Engineering and System Safety*, 121, 1–10. Open Access.
Aven, T. and Michiels van Kessenich, A. (2018) Teaching children and youths about risk and risk analysis: What are the goals and the risk analytical foundation? *Journal of Risk Research*. DOI: 10.1080/13669877.2018.1547785.
Aven, T. and Nøkland, T.E. (2010) On the use of uncertainty importance measures in reliability and risk analysis. *Reliability Engineering and System Safety*, 95, 127–33.
Aven, T. and Reniers, G. (2013) How to define and interpret a probability in a risk and safety setting. Discussion paper, with general introduction by Associate Editor, Genserik Reniers. *Safety Science*, 51, 223–31.
Aven, T. and Renn, O. (2009) On risk defined as an event where the outcome is uncertain. *Journal of Risk Research*, 12, 1–11.
Aven, T. and Renn, O. (2010) *Risk Management and Risk Governance*. Dordrecht: Springer Verlag.
Aven, T. and Renn, O. (2012) On the risk management and risk governance for petroleum operations in the Barents Sea area. *Risk Analysis*, 32(9), 1561–75.
Aven, T. and Renn, O. (2015) An evaluation of the treatment of risk and uncertainties in the IPCC reports on climate change. *Risk Analysis*, 35(4), 701–12. Open Access.
Aven, T. and Renn, O. (2018) Improving government policy on risk: Eight key principles. *Reliability Engineering and System Safety*, 176, 230–41.
Aven, T. and Renn, O. (2019) Some foundational issues related to risk governance and different types of risks. *Journal of Risk Research*. DOI: 10.1080/13669877.2019.1569099.
Aven, T., Renn, O. and Rosa, E. (2011) On the ontological status of the concept of risk. *Safety Science*, 49, 1074–9.
Aven, T. and Thekdi, S. (2018) The importance of resilience-based strategies in risk analysis, and vice versa. In B.D. Trump, M.-V. Florin and I. Linkov (eds), *IRGC Resource Guide on Resilience* (Vol. 2): *Domains of Resilience for Complex*

Interconnected Systems. Lausanne: EPFL International Risk Governance Center, 33–8. Available at: irgc.epfl.ch and irgc.org.

Aven, T. and Thekdi, S. (2019) *Enterprise Risk Management. Advances on its Foundation and Practice*. New York: Routledge.

Aven, T. and Vinnem, J.E. (2007) *Risk Management*. Berlin: Springer.

Aven, T. and Ylonen, M. (2016) Safety regulations: Implications of the new risk perspectives. *Reliability Engineering and System Safety*, 149, 164–71.

Aven, T. and Ylonen, M. (2018) The enigma of knowledge in the risk field. In T. Aven and E. Zio (eds), *Knowledge in Risk Assessments*, 27–48. New York: Wiley.

Aven, T. and Ylonen, M. (2019) The strong power of standards in the safety and risk fields: A threat to proper developments of these fields? *Reliability Engineering and System Safety*, 189, 279-86.

Aven, T. and Zio, E. (2013) Model output uncertainty in risk assessment. *International Journal of Performability Engineering IJPE*, 9(5), 475–86.

Aven, T. and Zio, E. (2014) Foundational issues in risk analysis. Risk Analysis, 34*(7)*, 1164–72.

Ayyub, B.M. (2014) *Risk Analysis in Engineering and Economics*. 2nd ed. New York: Chapman & Hall/CRC.

Bang, P. and Thuestad, O. (2014) Government-enforced self-regulation: The Norwegian case. In P. Lindøe, M. Baram and O. Renn (eds), *Risk Governance of Offshore Oil and Gas Operations*, 243–73. Cambridge, MA: Cambridge University Press.

Banks, E. and Dunn, R. (2003) *Practical Risk Management*. Chichester: Wiley.

Baram, M. (1980) Cost-benefit analysis: An inadequate basis for health, safety, and environmental regulatory decisionmaking. *Ecology Law Quarterly*, 8, 473–531.

Bayarri, M.J., Berger, J.O., Paulo, R., Sacks, J., Cafeo, J.A., Cavendish, J., Lin, C.H. and Tu, J. (2007) A framework for validation of computer models. *Technometrics*, 49(2), 138–54.

Beard, A.N. (2004) Risk assessment assumptions. *Civil Engineering and Environmental Systems*, 21(1), 19–31.

Beck, U. (1992) [1986] *Risk Society: Toward a New Modernity*, trans. Mark A. Ritter. London: Sage Publications.

Bedford, T. and Cooke, R. (2001) *Probabilistic Risk Analysis*. Cambridge: Cambridge University Press.

Bergman, B. (2009) Conceptualistic pragmatism: A framework for Bayesian analysis? *IIE Transactions*, 41, 86–93.

Bergman, B. and Klefsjö, B. (2003) *Quality*. 2nd ed. Lund: Studentlitteratur.

Bergström, J., Van Winsen, R. and Henriqson, E. (2015) On the rationale of resilience in the domain of safety: A literature review. *Reliability Engineering and System Safety*, 141, 131–41.

Berner, C.L. and Flage, R. (2016a) Strengthening quantitative risk assessments by systematic treatment of uncertain assumptions. *Reliability Engineering and System Safety*, 151, 46–59.

Berner, C. L. and Flage, R. (2016b) Comparing and integrating the NUSAP notational scheme with an uncertainty based risk perspective. *Reliability Engineering and System Safety*, 156, 185–94.

Berner, C.L. and Flage, R. (2017) Creating risk management strategies based on uncertain assumptions and aspects from assumption based planning. *Reliability Engineering and System Safety*, 167, 10–19.

Bhamra, R., Dani, S. and Burnard, K. (2011) Resilience: The concept, a literature review and future directions. *International Journal of Production Research*, 49(15), 5375–93.

Bier, V.M. (2001a) On the state of the art: Risk communication to decision-makers. *Reliability Engineering and System Safety*, 71, 151–7.

Bier, V.M. (2001b) On the state of the art: Risk communication to the public. *Reliability Engineering and System Safety*, 71, 139–50.

Bjerga, T. and Aven, T. (2015) Adaptive risk management using the new risk perspectives – an example from the oil and gas industry. *Reliability Engineering and System Safety*, 134, 75–82.

Bjerga, T. and Aven, T. (2016) Some perspectives on risk management – a security case study from the oil and gas industry. *Journal of Risk and Reliability*, 230(5), 512–20.

Bjerga, T., Aven, T. and Flage, R. (2018) Completeness uncertainty: Conceptual clarification and treatment. In T. Aven and E. Zio (eds), *Knowledge in Risk Assessment*, 127–42. New York: Wiley.

Bjerga, T., Aven, T. and Zio, E. (2014) An illustration of the use of an approach for treating model uncertainties in risk assessment. *Reliability Engineering and System Safety*, 125, 46–53.

Bjerga, T., Aven, T. and Zio, E. (2016) Uncertainty treatment in risk analysis of complex systems: The cases of STAMP and FRAM. *Reliability Engineering and System Safety*, 156, 203–9.

Bjørnsen, K. and Aven, T. (2016) Evaluating pre-accident risk assessments in accident investigations. In Proceedings from ESREL 2016, Glasgow.

Boholm, A. (1998) Comparative studies of risk perception: A review of twenty years of research. *Journal of Risk Research*, 1(2), 135–63.

Borgonovo, E. (2006) Measuring uncertainty importance: Investigation and comparison of alternative approaches. *Risk Analysis*, 26(5), 1349–61.

Bostrom, A. and Löfstedt, R.E. (2003) Communicating risk: Wireless and hardwired. *Risk Analysis*, 23(2), 241–8.

Bourdieu, P. and Wacquant, L.J.D. (1992) *An Invitation to Reflexive Sociology*. Chicago: University of Chicago Press.

Boyer-Kassem, T. (2017) Is the precautionary principle really incoherent? *Risk Analysis*, 37(11), 2026–34.

Brandtner, M. (2013) Conditional value-at-risk, spectral risk measures and (non-) diversification in portfolio selection problems: A comparison with mean–variance analysis. *Journal of Banking and Finance*, 37, 5526–37.

Brunsson, N., Rasche, A. and Seidl, D. (2012) The dynamics of standardization: Three perspectives on standards in organization studies. *Organization Studies*, 33(5–6), 613–32.

Chaiken, S. and Trope, Y. (1999) *Dual-Process Theories in Social Psychology*. New York: Guilford.

Charnley, G. and Elliott, E.D. (2000) Risk versus precaution: A false dichotomy. In M.P. Cottam, D.W. Harvey, R.P. Paper and J. Tait (eds), *Foresight and Precaution*, Vol. 1. Rotterdam and Brookfield: Balkema, 209–12.

Chichilnisky, G. (2013) The foundations of statistics with black swans. *Mathematical Social Sciences*, 59, 184–92.

Cojazzi, G. and Pinola, L. (1994) Root cause analysis methodologies: Trends and needs. In G.E. Apostolakis and J.S. Wu (eds), Proceedings of PSAM II, San Diego, CA, March 20–5.

Cooke, R.M. (1986) Conceptual fallacies in subjective probability. *Topoi*, 5, 21–8.
Cooke, R.M. (2004) The anatomy of the Squizzle – the role of operational definitions in science. *Reliability Engineering and System Safety*, 85, 313–19.
Copeland, T.E. and Weston, J.F. (1988) *Finance Theory and Corporate Policy*. 3rd ed. Addison-Wesley Publishing Co.
Council of Europe (2017) 12 Principles of Good Governance. https://www.coe.int/en/web/good-governance/12-principles-and-eloge?desktop=true. Accessed Sept. 2017.
Covello, V., von Winterfeldt, D. and Slovic, P. (1986) Risk communication: A review of the literature. *Risk Abstracts*, 3(4), 171–82.
Cox, L.A., Jr. (2011) Clarifying types of uncertainty: When are models accurate, and uncertainties small? *Risk Analysis*, 31, 1530–3.
Cox, L.A., Jr. (2012) Confronting deep uncertainties in risk analysis. *Risk Analysis*, 3, 1607–29.
Cox, L.A., Jr., Popken, D.A and Sun, R.X. (2018) *Causal Analytics for Applied Risk Analysis*. Cham, Switzerland: Springer.
Cumming, R.B. (1981) Is risk assessment a science? *Risk Analysis*, 1, 1–3.
Curt, C. and Tacnet, J.-M. (2018) Resilience of critical infrastructures: Review and analysis of current approaches. *Risk Analysis*, 38(11), 2441–58.
de Finetti, B. (1937) La prévision: Ses lois logiques, ses sources subjectives. *Annales de l'Institut Henri Poincaré*, 7(1), 1–68.
Delogu, B. (2016) *Risk Analysis and Governance in EU Policy Making and Regulation. An Introductory Guide*. Heidelberg and Zurich: Springer.
De Marchi, B. (2015) Risk governance and the integration of different types of knowledge. In U. Fra Paleo (ed.), *Risk Governance. The Articulation of Hazard, Politics and Ecology*. Heidelberg and New York: Springer, 149–66.
Deming, W.E. (2000) *The New Economics*. 2nd ed. Cambridge, MA: MIT CAES.
Devooght, J. (1998) Model uncertainty and model inaccuracy. *Reliability Engineering and System Safety*, 59, 171–85.
Dewar, J.A. (2002) *Assumption-Based Planning: A Tool for Reducing Avoidable Surprises*. Cambridge: Cambridge University Press.
Dinh, L.T.T., Pasman, H., Gao, X. and Mannan, M.S. (2012) Resilience engineering of industrial processes: Principles and contributing factors. *Journal of Loss Prevention in the Process Industries*, 25, 233–41.
Douglas, M. and Wildavsky, A. (1982) *Risk and Culture: The Selection of Technological and Environmental Dangers*. Berkeley, CA: University of California Press.
Dowdle, W.R. (2006) Influenza pandemic periodicity, virus recycling, and the art of risk assessment. *Emerging Infectious Disease*, 12(1), 34–9.
Droguett, E.L. and Mosleh, A. (2008) Bayesian methodology for model uncertainty using model performance data. *Risk Analysis*, 28(5), 1457–76.
Droguett, E.L. and Mosleh, A. (2014) Bayesian treatment of model uncertainty for partially applicable models. *Risk Analysis*, 34(2), 252–70.
Dubois, D. (2010) Representation, propagation and decision issues in risk analysis under incomplete probabilistic information. *Risk Analysis*, 30, 361–8.
Edwards, W. and von Winterfeldt, D. (1987) Public values in risk debates. *Risk Analysis*, 7, 141–58.
EFSA (2016) *Guidance on Uncertainty in EFSA (European Food Safety Authority) Scientific Assessment: Revised Draft for Internal Testing*. Parma: EFSA. https://www.efsa.europa.eu/sites/default/files/160321DraftGDUncertaintyInScientificAssessment.pdf. Accessed May 2017.

Epstein, S. (1994) Integration of the cognitive and the psychodynamic unconscious. *American Psychologist*, 49, 709–24.

Ethik-Kommission (2011) *Deutschlands Energiewende. Ein Gemeinschaftswerk für die Zukunft*. Berlin: Endbericht.

Feduzi, A. and Runde, J. (2014) Uncovering unknown unknowns: Towards a Baconian approach to management decision-making. *Organizational Behavior and Human Decision Processes*, 124, 268–83.

Feleppa, R. (1981) Epistemic utility and theory acceptance: Comments on Hempel. *Synthese*, 46, 413–20.

Fischhoff, B. (1985) Managing risk perceptions. *Issues in Science and Technology*, 2(1), 83–96.

Fischhoff, B., Slavic, P., Lichtenstein, S., Read, S. and Combs, B. (1978) How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Sciences*, 9, 127–52.

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

Fischhoff, B. (1995) Risk perception and communication unplugged: Twenty years of process. *Risk Analysis*, 15, 137–45.

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

Fischhoff, G., Goitein, B. and Shapiro, Z. (1982) The experienced utility of expected utility approaches. In N.T. Feather (ed.), *Expectations and Actions: Expectancy-Value Models in Psychology*. Hillsdale NJ: Lawrence Erlbaum, 315–40.

Fishbein, W. and Trevorton, G. (2004) *Rethinking Alternative Analysis to Address Transnational Threats*. Occasional Papers, 3(2). Wasahington, DC: Sherman Kent Center for Intelligence Analysis.

Flach, F.F. (1988) *Resilience: Discovering a New Strength at Times of Stress*. New York: Fawcett Columbine.

Flage, R. and Aven, T. (2009) Expressing and communicating uncertainty in relation to quantitative risk analysis (QRA). *Reliability and Risk Analysis: Theory and Applications*, 2(13), 9–18.

Flage, R. and Aven, T. (2015) Emerging risk – conceptual definition and a relation to black swan types of events. *Reliability Engineering and System Safety*, 144, 61–7.

Flage, R., Aven, T., Baraldi, P. and Zio, E. (2014) Concerns, challenges and directions of development for the issue of representing uncertainty in risk assessment. *Risk Analysis*, 34(7), 1196–1207.

Flage, R., Aven, T. and Berner, C.L. (2018) A comparison between a probability bounds analysis and a subjective probability approach to express epistemic uncertainties in a risk assessment context – a simple illustrative example. *Reliability Engineering and System Safety*, 169, 1–10.

Flanders, W.D., Lally, C.A., Zhu, B-P., Henley, S.J. and Thun, M.J. (2003) Lung cancer mortality in relation to age, duration of smoking, and daily cigarette consumption. *Cancer Research*, 63, 6556–62.

Flyvbjerg, B. (2006) Five misunderstandings about case-study research. *Qualitative Inquiry*, 12(2), 219–45.

Ford, E., Aven, T., Røed, W. and Wiencke, H.S. (2008) An approach for evaluating methods for risk and vulnerability assessments. *Journal of Risk and Reliability*, 220, 315–26.

Francis, R. and Bekera, B. (2014) A metric and framework for resilience analysis of engineered and infrastructure system. *Reliability Engineering and System Safety*, 121, 90–103.

Free (2018) https://www.thefreedictionary.com/ambiguity. Accessed Oct. 2018.

French, S., Bedford, T. and Atherton, E. (2005) Supporting ALARP decision-making by cost benefit analysis and multiattribute utility theory. *Journal of Risk Research*, 8(3), 2017–2223.

Freudenburg, W.R. (1989) Perceived risk, real risk: Social science and the art of probabilistic risk assessment. *Science*, 242, 44–9.

Frewer, L.J., Miles, S., Brennan, M., Kusenof, S., Ness, M. and Ritson, C. (2002) Public preferences for informed choice under conditions of risk uncertainty. *Public Understanding of Science*, 11(4), 1–10.

Fuchs, C. (2005) Science as a self-organizing meta-information system. In I. Dobronravova and W. Hofkirchner (eds), *Science of Self-Organization and Self-Organization of Science*. Kiev: Abris, 126–99. ISBN 966-531-165-4.

Funtowicz, S.O. and Ravetz, J.R. (1985) Three types of risk assessment. In C. Whipple and V.T. Covello (eds), *Risk Analysis in the Private Sector*. New York: Plenum Press, 217–31.

Funtowicz, S.O. and Ravetz, J.R. (1990) *Uncertainty and Quality in Science for Policy*. Dordrecht: Kluwer Academic Publishers.

Funtowicz, S.O. and Ravetz, J.R. (1993) Science for the post-normal age. *Futures*, 25, 735–55.

Funtowicz, S.O. and Ravetz, J.R. (1994) The worth of a songbird: Ecological economics as a postnormal science. *Ecological Economics*, 10, 197–207.

Funtowicz, S.O. and Strand, R. (2007) Models of science and policy. In T. Traavik and L.C. Lim (eds), *Biosafety First: Holistic Approaches to Risk and Uncertainty in Genetic Engineering and Genetically Modified Organisms*. Trondheim: Tapir Academic Press.

Gilboa, I. and Marinacci, M. (2013) Ambiguity and the Bayesian paradigm. In D. Acemoglu, M. Arellano and E. Dekel (eds), *Advances in Economics and Econometrics: Theory and Applications*. Cambridge: Cambridge University Press.

Goerlandt, F., Khakzad, N. and Reniers, G. (2017) Validity and validation of safety-related quantitative risk analysis: A review. *Safety Science*, 99B, 127–39.

Gourlay, S. (2001) Knowledge management and HRD. *Human Resource Development International*, 4(1), 27–46.

Graham, J., Amos, B. and Plumptre, T. (2003) *Principles for Good Governance in the 21st Century*. Policy Brief No. 15, Aug. http://unpan1.un.org/intradoc/groups/public/documents/UNPAN/UNPAN011842.pdf. Accessed Sept. 2017.

Greenberg, M., Goldstein, B.D., Andersen, E., Doursen, M., Landis, W. and North, D.W. (2015) Whither risk assessment: New challenges and opportunities a third of a century after the Red Book. *Risk Analysis*, 35(11), 1959–68.

Greenberg, M.R. (2017) *Explaining Risk Analysis*. New York: Earthscan.

Gregersen, E. (ed.) (2011) *The Britannica Guide to Statistics and Probability*. New York: The Britannica Educational Publishing, 115.

Gross, M. (2010) *Ignorance and Surprises*. London: MIT Press.

Haimes, Y.Y. (2009) On the definition of resilience in systems. *Risk Analysis*, 29, 498–501.

Haimes, Y.Y. (2015) *Risk Modeling, Assessment, and Management*. 4th ed. New York: Wiley.

Hale, A. (2015) Advancing robust regulation: Reflections and lessons to be learned. In P.H. Lindoe, M. Baram and O. Renn (eds), *Risk Governance of Offshore Oil and Gas Operations*. New York: Cambridge University Press, 403–24.

Hammerlin J. (2009) *Terrorindustrien*. Oslo: Manifest [in Norwegian].

Hammitt, J.K., Wiener, J.B., Swedlow, B., Kall, D. and Zhou, Z. (2005) Precautionary regulation in Europe and the United States: A quantitative comparison. *Risk Analysis*, 25, 1215–28.

Hanley, N. and Spash, C.L. (1993) *Cost-benefit Analysis and the Environment*. Cheltenham: Edward Elgar.

Hansson, S.O. (2013a) Defining pseudoscience and science. In M. Pigliucci and M. Boudry (eds), *Philosophy of Pseudoscience*. Chicago: University of Chicago Press, 61–77.

Hansson, S.O. (2013b) *The Ethics of Risk*. New York: Palgrave-Macmillan.

Hansson, S.O. and Aven, T. (2014) Is risk analysis scientific? *Risk Analysis*, 34(7), 1173–83.

Harrison, M. (2010) *Valuing the Future: The Social Discount Rate in Cost-Benefit Analysis*. https://www.pc.gov.au/research/supporting/cost-benefit-discount/cost-benefit-discount.pdf. Accessed Nov. 2018.

Harvey, C. (2018) The EAT 'Broken Links' approach: Assessing risks in sociotechnical systems. In N.D. Stanton, P. D. Salmon and G.D. Walker (eds), *Systems Thinking in Practice*. Boca Raton, FL: CRC Press, 23–42.

Haugen, S., and Vinnem, J.E. (2015) Perspectives on risk and the unforeseen. *Reliability Engineering and System Safety*, 137, 1–5.

Heckmann, I., Comes, T. and Nickel, S. (2015) A critical review on supply chain risk: Definition, measure and modeling. *Omega*, 52, 119–32.

Helsloot, I. and Ruitenberg, A. (2004) Citizen response to disaster: A survey of literature and some practical implications. *Journal of Contingencies and Crisis Management*, 12(3), 98–111.

Helton, J.C., Johnson, J.D. and Oberkampf, W.L. (2004) An exploration of alternative approaches to the representation of uncertainty in model predictions. *Reliability Engineering and System Safety*, 85(1–3), 39–71.

Hempel, C.G. (1960) Inductive inconsistencies. *Synthese*, 12, 439–69.

Hertz, D.B. and Thomas, H. (1983) *Risk Analysis and its Applications*. Chichester: Wiley.

Heuer, R.J. and Pherson, R.H. (2010) *Structured Analytic Techniques for Intelligence Analysis*. Washington, DC: CQ Press.

HMSO (1988) *The Tolerability of Risk from Nuclear Power Stations*. London: Health and Safety Executive.

Holling, C.S. (1973) Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, 4(1), 1–23.

Hollnagel, E. (2004) *Barriers and Accident Prevention*. Aldershot, Surrey: Ashgate.

Hollnagel, E. (2010) Prologue: The scope of resilience engineering. In E. Hollnagel, J. Paries, D.D. Woods and J. Wreathall (eds), *Resilience Engineering in Practice: A Guidebook*, pp. xxx–xxxix. Boca Raton, FL: Ashgate Publishing Co.

Hollnagel, E. (2012) *FRAM, the Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems*. Aldershot, Surrey: Ashgate.

Hollnagel, E., Woods, D. and Leveson, N. (2006) *Resilience Engineering: Concepts and Precepts*. Surrey: Ashgate.

Hood, C., Rothstein, H. and Baldwin, R. (2001) *The Government of Risk: Understanding Risk Regulation Regimes*. Oxford: Oxford University Press.

Hopkin, P. (2010) *Fundamentals of Risk Management*. London: The Institute of Risk Management.

Hosseini, S., Barker, K. and Ramirez-Marquez, J.E. (2016) A review of definitions and measures of system resilience. *Reliability Engineering and System Safety*, 145, 47–61.

Hudson, R.G. (1994) Reliability, pragmatic and epistemic. *Erkenntnis*, 40(1), 71–86.

IPCC (2007) *IPCC Climate Change 2007: Synthesis Report*. Contribution of Working Groups I, II and III to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change. Core Writing Team, R.K. Pachauri and A. Reisinger. Geneva: IPCC, 104.

IPCC (2010) *Guidance Notes for Lead Authors of the IPCC Fifth Assessment Report on Consistent Treatment of Uncertainties*. Geneva: IPCC Cross Working Group Meeting on Consistent Treatment of Uncertainties.

IPCC (2014a) *Climate Change 2014 Synthesis Report Summary for Policymakers*. https://www.ipcc.ch/pdf/assessment-report/ar5/syr/AR5_SYR_FINAL_SPM.pdf. Accessed July 2018.

IPCC (2014b) *IPCC Climate Change 2014: Impacts, Adaptation, and Vulnerability*. WGII AR5 Technical Summary. Accessed July 2018.

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

ISO (2016) *Petroleum and Natural Gas Industries: Offshore Production Installations. Major Accident Hazard Management during the Design of New Installations*. ISO 17776. Geneva: ISO.

ISO (2018) *Risk Management Guidelines*. ISO/FDIS 31000:2017(E). Geneva: ISO.

Jasanoff, S. (1999) The songlines of risk. *Environmental Values*. Special Issue: *Risk*, 8(2), 135–52.

Jensen, A. and Aven, T. (2018) A new definition of complexity in a risk analysis setting. *Reliability Engineering and System Safety*, 171, 169–173.

Jiang, X., Yang, R.J., Barbat, S. and Weerappuli, P. (2009) Bayesian probabilistic PCA approach for model validation of dynamic systems. Proceedings of SAE World Congress and Exhibition, Detroit, MI, April.

Johansen, I.L. and Rausand, M. (2015) Ambiguity in risk assessments. *Safety Science*, 80, 243–51.

Jones-Lee, M. and Aven, T. (2009) The role of social cost-benefit analysis in societal decision-making under large uncertainties with application to robbery at a cash depot. *Reliability Engineering and System Safety*, 94, 1954–61.

Josephson, M. (2002) *Making Ethical Decisions*. Los Angeles, CA: Josephson Institute. https://store.charactercounts.org/wp-content/uploads/sites/10/2015/09/50-0450-E.pdf. Accessed July 2018.

Kahneman, D. (2011) *Thinking, Fast and Slow*. New York: Farrar, Straus & Giroux.

Kahneman, D. and Frederick, S. (2002) Representativeness revisited: Attribute substitution in intuitive judgment. In T. Gilovich, D. Griffin and D. Kahneman (eds), *Heuristics and Biases: The Psychology of Intuitive Judgment*. New York: Cambridge University Press, 49–81.

Kahneman, D., Slovic, P. and Tversky, A. (1982) *Judgment under Uncertainty: Heuristics and Biases*. Cambridge: Cambridge University Press.

Kaminski Jr., J., Riera, J.D., de Menezes, R.C.R. and Miguel, L.F.F. (2008) Model uncertainty in the assessment of transmission line towers subjected to cable rupture. *Engineering Structures*, 30, 2935–44.

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

Kaplan, S., Visnepolschi, S., Zlotin, B. and Zusman, A. (1999) *New Tools for Failure and Risk Analysis: Anticipatory Failure Determination (AFD) and the Theory of Scenario Structuring*. Southfield, MI: Ideation International Inc.

Karvetski, C.W. and Lambert, J.H. (2012) Evaluating deep uncertainties in strategic priority-setting with an application to facility energy investments. *Systems Engineering*, 15(4), 483–93.

Kasperson, R.E. (1992) The social amplification of risk – progress in developing an integrative framework. In S. Krimsky and D. Golding (eds), *Social Theories of Risk*. Westport CT: Praeger, 153–78.

Kasperson, R.E., Renn, O., Slovic, P., Brown, H.S., Ernel, J., Goble, R., Kasperson, J.S. and Ratick, S. (1988) The social amplification of risk: A conceptual framework. *Risk Analysis*, 8, 177–87.

Kaufman, G. and Scott, K.E. (2003) What is systemic risk, and do bank regulators retard or contribute to it? *The Independent Review*, 7(3), 371–91.

Keeney, R.L. and von Winterfeldt, D. (1986) Improving risk communication. *Risk Analysis*, 6, 417–24.

Keller, C., Siegrist, M. and Gutscher, H. (2006) The role of the affect and availability heuristics in risk communication. *Risk Analysis*, 26(3), 631–9.

Kennedy, M. C. and O'Hagan, A. (2001) Bayesian calibration of computer models. *Journal of the Royal Statistical Society*, Series B (Statistical Methodology), 63(3), 425–64.

Khan, F., Rathnayaka, S. and Ahmed, S. (2015) Methods and models in process safety and risk management: Past, present and future. *Process Safety and Environmental Protection*, 98, 116–47.

Khorsandi, J. and Aven, T. (2017) Incorporating assumption deviation risk in Quantitative Risk Assessments: A semi-quantitative approach. *Reliability Engineering and System Safety*, 163, 22–32.

Khorsandi, J., Aven, T. and Vinnem, J.E. (2012) A review and discussion of the Norwegian Offshore Safety Regulation Regime for Risk Assessments. PSAM 11-ESREL 2012, 25–9 July, Helsinki.

Kirwan, B., Hale, A. and Hopkins, A. (eds) (2002) *Changing Regulations*. Oxford: Pergamon Press.

Klinke, A. and Renn, O. (2001) Precautionary principle and discursive strategies: Classifying and managing risks. *Journal of Risk Research*, 4(2), 159–74.

Klinke, A. and Renn, O. (2002) A new approach to risk evaluation and management: Risk-based precaution-based and discourse-based strategies. *Risk Analysis*, 22(6), 1071–94.

Klinke, A. and Renn, O. (2012) Adaptive and integrative governance on risk and uncertainty. *Journal of Risk Research*, 15(3), 273–92.

Kloprogge, P., van der Sluijs, J. and Petersen, A. (2005) *A Method for the Analysis of Assumptions in Assessments*. Bilthoven, the Netherlands: Netherlands Environmental Assessment Agency (MNP).

Kloprogge, P., van der Sluijs, J.P. and Petersen, A.C. (2011) A method for the analysis of assumptions in model-based environmental assessments. *Environmental Modelling and Software*, 26, 289–301.

Knupp, P. (2002) *Verification of Computer Codes in Computational Science and Engineering*. Boca Raton, FL: Chapman & Hall/CRC.

Kothari, C.R. (2004) *Research Methodology*. New Delhi: New Age International Publishers.

Krieger, K. (2013) The limits and variety of risk-based governance: The case of flood management in Germany and England. *Regulation and Governance*, 7(2), 236–57.

Lacey, H. (2015) 'Holding' and 'endorsing' claims in the course of scientific activities. *Studies in History and Philosophy of Science*, 50 (Oct.), 89–95.

Laes, E., Meskens, G. and van der Sluijs, J.P. (2011) On the contribution of external cost calculations to energy system governance: The case of a potential large-scale nuclear accident. *Energy Policy*, 39, 5664–73.

Lambert, J.H., Karvetski, C.W., Spencer, D.K., Sotirin, B.J., Liberi, D.M., Zaghloul, H.H., Koogler, J.B., Hunter, S.L., Goran, W.D., Ditmer, R.D. and Linkov, I. (2012) Prioritizing infrastructure investments in Afghanistan with multiagency stakeholders and deep uncertainty of emergent conditions. *ASCE Journal of Infrastructure Systems*, 18(2), 155–66.

Le Coze, J.C. (2016) Vive la diversité! High Reliability Organisation (HRO) and Resilience Engineering (RE). *Safety Science*. 10.1016/j.ssci.2016.04.006.

Leveson, N. (2004) A new accident model for engineering safer systems. *Safety Science*, 42(4), 237–70.

Leveson, N. (2011) *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, MA: MIT Press.

Lewis, C.I. (1929) *Mind and the World Order: Outline of a Theory of Knowledge*. New York: Dover Publications.

Lincoln, Y.S. and Guba, E.G. (2000) Paradigmatic controversies, contradictions, and emerging confluences. In N.K. Denzin and Y.S. Lincoln (eds), *Handbook of Qualitative Research*. 2nd ed. Thousand Oaks, CA: Sage Publications, 163–88.

Lindley, D.V. (1970) *Introduction to Probability and Statistics from a Bayesian Viewpoint*. Cambridge: Cambridge University Press.

Lindley, D.V. (1985) *Making Decisions*. New York: Wiley.

Lindley, D.V. (2000) The philosophy of statistics. *The Statistician*, 49, 293–337. With discussions.

Lindley, D.V. (2006) *Understanding Uncertainty*. Hoboken, NJ: Wiley.

Lindøe, P. and Engen, O.A. (2013) Offshore safety regimes: A contested terrain. In M. Nordquist, J.N. More, A. Chircop and R. Long (eds), *The Regulation of Continental Shelf Development. Rethinking International Standards*. Leiden: Martinus Nijhoff.

Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., Lambert, J.H., Levermann, A., Montreuil, B., Nathwani, J., Nyer, R., Renn, O., Scharte, B., Scheffler, A., Schreurs, M. and Thiel-Clemen, T. (2014) Changing the resilience paradigm. *Nature Climate Change*, 4, 407–9.

Linkov, I., Trump, B.D. and Fox-Lent, C. (2016) Resilience: Approaches to risk analysis and governance. An introduction to the IRGC Resource Guide on Resilience. In I. Linkov and M.-V. Florin (eds), *IRGC Resource Guide on Resilience*. Lausanne: IRGC.

Löfstedt, R.(2003) The precautionary principle: Risk, regulation and politics. *Process Safety and Environmental Protection*, 81(1), 36–43.

Löfstedt, R. and Bouder, F. (2017) Evidence-based uncertainty analysis: What should we now do in Europe? A view point. *Journal of Risk Research*. https://doi.org/10.1080/13669877.2017.1316763.

Löfstedt, R. and Vogel, D. (2001) The changing character of regulation: A comparison of Europe and the United States. *Risk Analysis*, 21, 399–405.

McComas, K.A. (2006) Defining moments in risk communication research: 1996–2005. *Journal of Health Communication*, 11(1), 75–91.

MacInnis, D.J. (2011) A framework for conceptual contributions in marketing. *Journal of Marketing*, 75(4), 136–54.

Mannheim, K. (1979) *Ideology and Utopia: An Introduction to the Sociology of Knowledge*. London: Routledge & Kegan Paul. Original (1936).

March, J.G. and Shapira, Z. (1987) Managerial perspectives on risk and risk taking. *Management Science*, 33(11), 1404–18.

Martin, R. (2009) *The Opposable Mind*. Boston, MA: Harvard Business Press.

Masys, A.J. (2012) Black swans to grey swans: Revealing the uncertainty. *Disaster Prevention and Management*, 21(3), 320–35.

Mearns, K. (2015) Values and norms: A basis for safety culture. In P.H. Lindoe, M. Baram and O. Renn (eds), *Risk Governance of Offshore Oil and Gas Operations*. New York: Cambridge University Press, 56–77.

Meeker, W.O. and Escobar, L.A. (1998) *Statistical Methods for Reliability Data*. New York: Wiley.

Mennen, M.G. and van Tuyll, M.C. (2015) Dealing with future risks in the Netherlands: The National Security Strategy and the National Risk Assessment. *Journal of Risk Research*, 18(7), 860–76.

Merton, R.K. (1973) Science and technology in a democratic order. *Journal of Legal and Political Sociology*, 1942(1), 115–26. Reprinted as The normative structure of science. In R.K. Merton, *The Sociology of Science. Theoretical and Empirical Investigations*. Chicago: University of Chicago Press, 267–78.

Metzger, M.B. (2010) Problems with probabilities. *Business Horizons*, 53, 15–19.

Meyer, T. and Reniers, G. (2013) *Engineering Risk Management*. Berlin: De Gruyter Graduate.

MI & E (2014) Explicitly dealing with safety: General principles. Ministry of Infrastructure and Environment. July 2014, file:///C:/Users/Eier/AppData/Local/Packages/microsoft.windowscommunicationsapps_8wekyb3d8bbwe/LocalState/Files/S0/12822/93243_Brochure_rode_draden_ENG[18701].pdf. Accessed Apr. 2017.

Miller, B. (2013) When is consensus knowledge-based? Distinguishing shared knowledge from mere agreement. Synthese, 190, 1293–1316.

Mitra, S., Karathanasopoulos, A., Sermpinis, G., Christian, D. and Hood, J. (2015) Operational risk: Emerging markets, sectors and measurement. *European Journal of Operational Research*, 241, 122–32.

Mohaghegh, Z., Kazemi, R. and Mosleh, A. (2009) Incorporating organizational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: A hybrid technique formalization, *Reliability Engineering and System Safety*, 94, 1000–18.

Morse, J.M., Mitcham, C., Hupcey, J.E. and Tason, M.C. (1996) Criteria for concept evaluation. *Journal of Advanced Nursing*, 24(2), 385–90.

Moser, S.A. (2010) Communicating climate change: History, challenges, process and future directions. *WIREs Climate Change*, 1(1), 31–53.

Munsterhjelm-Ahumada, K. (2012) Health authorities now admit severe side effects of vaccination swine flu, pandemrix and narcolepsy. Orthomolecular Medicine News Service, March 20. http://orthomolecular.org/resources/omns/v08n10.shtml. Accessed May 2018.

Natarajan, K., Pachamanova, D. and Sim, M. (2009) Constructing risk measures from uncertainty sets. *Operations Research*, 57(5), 1129–41.

NC (2011) *Deepwater: The Gulf Oil Disaster and the Future of Offshore Drilling*. Report to the President 11 Jan. Washington, DC: National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling.

Nilsen, T. and Aven, T. (2003) Models and model uncertainty in the context of risk analysis. *Reliability Engineering and System Safety*, 79, 309–17.

NOG (2017) Black swan. Norwegian Oil and Gas Association. https://www.norskoljeoggass.no/en/Publica/HSE-and-operations/Black-swans/. Accessed July 2018.

North, W.D. (2011) Uncertainties, precaution, and science: Focus on the state of knowledge and how it may change. *Risk Analysis*, 31, 1526–9.

NRC (1975) *Reactor Safety Study, an Assessment of Accident Risks*. Wash 1400. Report NUREG-75/014. Washington, DC: US Nuclear Regulatory Commission.

NRC (2009) *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant Specific Changes to the Licensing Basis*. Regulatory Guide DG-1226, Proposed Revision of Regulatory Guide 1174, Washington, DC: US Nuclear Regulatory Commission, 1–34.

NUREG (2013) Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision-making. Draft Report for Comment. file:///C:/Users/Eier/Documents/papers2015/nureg-ML13093A346.pdf. Accessed July 2018.

Oberkampf, W. and Trucano, T. (2002) *Verification and Validation in Computational Fluid Dynamics*. Technical Report SAND2002-0529. Albuquerque, NM: Sandia National Laboratories.

O'Brien, M. (2000) *Making Better Environmental Decisions*. Cambridge, MA: MIT Press.

OECD (2003) *Emerging Systemic Risks: Final Report to the OECD Futures Project*. Paris: Organization for Economic Cooperation and Development.

OECD (2009) *OECD Studies in Risk Management: Innovation in Country Risk Management*. Paris: Organization for Economic Co-operation and Development. https://www.mmc.com/content/dam/mmc-web/Files/Innovation-in-Country-Risk-Management-2009.pdf. Accessed Apr. 2018.

OECD (2017) Risk and Regulatory Policy. http://www.oecd.org/gov/regulatory-policy/risk.htm. Accessed Apr. 2017.

OECD (2018) National Risk Assessments: A Cross Country Perspective. http://www.oecd.org/gov/national-risk-assessments-9789264287532-en.htm. Accessed April 16, 2018.

Omdal, S.E. (2009) Dominer! Skrem! Kontroller! *Stavanger Aftenblad*, 22 May. http://www.aftenbladet.no/energi/kommentar/Dominer-Skrem-Kontroller-2042227.html [in Norwegian] accessed Jan. 2019.

Östergaard, C., Dogliani, M., Guedes Soares, C., Parmentier, G. and Pedersen, P.T. (1996) Measures of model uncertainty in the assessment of primary stresses in ship structures. *Marine Structures*, 9, 427–47.

Park, J., Seager, T.P., Rao, P.S.C., Convertino, M. and Linkov, I. (2013) Integrating risk and resilience approaches to catastrophe management in engineering systems. *Risk Analysis*, 33(3), 356–67.

Parry, G. and Drouin, M.T. (2009) *Risk-Informed Regulatory Decision-Making at the U.S. NRC: Dealing with Model Uncertainty*. Washington, DC: Nuclear Regulatory Commission.

Pasman, H. and Reniers, G. (2014) Past, present and future of Quantitative Risk Assessment (QRA) and the incentive it obtained from Land-Use Planning (LUP). *Journal of Loss Prevention in the Process Industries*, 28, 2–9.

Pasman, H.J., Rogers, W.J. and Mannan, M.S. (2017) Risk assessment: What is it worth? Shall we just do away with it, or can it do a better job? *Safety Science*, 99(B), 140–55.

Paté, E. (1983) Acceptable decision processes and acceptable risk in public sector regulations. *IEEE Transactions on Systems. Man and Cybernetics*, 13(3), 113–24.

Paté-Cornell, M. (1996) Uncertainties in risk analysis: Six levels of treatment. *Reliability Engineering and System Safety*, 54(2–3), 95–111.

Paté-Cornell, E. (1999) Conditional uncertainty analysis and implications for decision making: The case of WIPP. *Risk Analysis*, 19, 995–1003.

Paté-Cornell, E. (2012) On "black swans" and "perfect storms": Risk analysis and management when statistics are not enough. *Risk Analysis*, 32, 1823–33.

Patriarca, R., Bergström, J., Gravio, G. Di and Costantino, F. (2018) Resilience engineering: Current status of the research and future challenges. *Safety Science*, 102, 79–100.

Perhac, R.M. Jr. (1996) Does risk aversion make a case for conservatism? *Risk: Health, Safety and Environment*, 7, 297.

Peterson, M. (2006) The precautionary principle is incoherent. *Risk Analysis*, 26(3), 595–601.

Peterson, M. (2007) The precautionary principle should not be used as a basis for decision-making. Talking Point on the precautionary principle. *EMBO Reports*, 8(4), 305–8.

Pfanzagl, J. (1968) *Theory of Measurement*. Würzburg-Wien Germany: Physica-Verlag.

Pidgeon, N.F. (1997) The limits to safety? Culture, politics, learning and manmade disasters. *Journal of Contingencies and Crisis Management*, 5(1), 1–14.

Pidgeon, P. (1998) Risk assessment, risk values and societal science programme: Why we do need risk perception research? *Reliability Engineering and System Safety*, 59, 5–15.

Pidgeon, N. and Fischhoff, B. (2011) The role of social and decision sciences in communicating uncertain climate risks. *Nature Climate Change*, 1, 35–41.

Pierre, J. and Peters, B.G. (2000) *Governance, Politics and the State*. Houndsmill/London: Macmillan.

Popper, K. (1962) *Conjectures and Refutations. The Growth of Scientific Knowledge*. New York: Basic Books.

Powell, D.A. and Leiss, W. (1997) *Mad Cows and Mother's Milk: The Perils of Poor Risk Communication*. Montreal: McGill–Queen's University Press.

Pritchard, C.L. (2015) *Risk Management: Concepts and Guidance*. 5th ed. New York: Auerbach.

Proctor, R.N. (2011) The history of the discovery of the cigarette–lung cancer link: Evidentiary traditions, corporate denial, global toll. *Tobacco Control*, 21, 87–91.

Pruyt, E. and Wijnmalen, D. (2010) National risk assessment in the Netherlands: A multi-criteria decision analysis approach. In M. Ehrgott, B. Naujoks, T. Stewart and J. Wallenius (eds), *Multiple Criteria Decision Making for Sustainable Energy and Transportation Systems*, Lecture Notes in Economics and Mathematical Systems. Berlin, Heidelberg: Springer Physica-Verlag, 133–43.

PSA-N (2012) *Report Following the Investigation of the Hydrocarbon Leakage on Heimdal 26.5.2012*. Stavanger: Petroleum Safety Authority Norway.

PSA-N (2013) *Report Following the Investigation of the Hydrocarbon Leakage on Ula P Platform 12.9.2012*. Stavanger: Petroleum Safety Authority Norway.
PSA-N (2018a) Petroleum Safety Authority Norway. https://www.ptil.no/en/regulations/all-acts/the-framework-regulations2/II/11/. Accessed May 2019.
PSA-N (2018b) Petroleum Safety Authority Norway. Risk level project. http://www.psa.no/risk-level/category876.html. Accessed Dec. 2018.
PST (2018) Norwegian Police Security Services (PST). Threat assessment 1018. https://pst.no/globalassets/artikler/trusselvurderinger/annual-threat-assessment-2018.pdf. Accessed Mar. 2018.
Quarantelli, E.L. (1993) Community crises: An exploratory comparison of the characteristics and consequences of disasters and riots. *Journal of Contingencies and Crisis Management*, 1(2), 61–78.
Rae, A., Alexander, R. and McDermid, J. (2014) Fixing the cracks in the crystal ball: A maturity model for quantitative risk assessment. *Reliability Engineering and System Safety*, 125, 67–81.
Ramsey, F.P. (1931, 2001) *The Foundations of Mathematics*. New York: Routledge. file:///C:/Users/Eier/Downloads/9781134528035_googlepreview.pdf. Accessed Oct. 2018.
Rasche, A. (2010) The limits of corporate responsibility standards. *Business Ethics: A European Review*, 19(3), 280–91.
Ravetz, J.R. and Funtowicz, S.O. (1999) Post-normal science: An insight now maturing. *Futures*, 31(7), 641–6.
Rayner, S. (1992) Cultural theory and risk analysis. In S. Krimsky and D. Golding (eds), *Social Theories of Risk*. Westport CT: Praeger, 83–115.
Rayner, S. and Cantor, R. (1987) How fair is safe enough? The cultural approach to societal technology choice. *Risk Analysis*, 7, 3–13.
Rebba, R., Mahadevan, S. and Huang, S. (2006) Validation and error estimation of computational models. *Reliability Engineering and System Safety*, 91, 1390–7.
Rechard, R.P. (1999) Historical relationship between performance assessment for radioactive waste disposal and other types of risk assessment. *Risk Analysis*, 19(5), 763–807.
Rechard, R.P. (2000) Historical background on performance assessment for the waste isolation pilot plant. *Reliability Engineering and System Safety*, 69(3), 5–46.
Reid, S.G. (1992) Acceptable risk. In D.I. Blockley (ed.), *Engineering Safety*. New York: McGraw-Hill, 138–66.
Reinert, J.M. and Apostolakis, G.E. (2006) Including model uncertainty in risk-informed decision making. *Annals of Nuclear Energy*, 33(4) 354–69.
Renn, O. (1998a) The role of risk communication and public dialogue for improving risk management. *Risk Decision and Policy*, 3, 5–30.
Renn, O. (1998b) Three decades of risk research: Accomplishments and new challenges. *Journal of Risk Research*, 1(1), 49–71.
Renn, O. (2008) *Risk Governance: Coping with Uncertainty in a Complex World*. London: Earthscan.
Renn, O. (2009) Precaution and the governance of risk. In N. Adger and A. Jordan (eds), *Governing Sustainability*. Cambridge, MA: Cambridge University Press, 226–58.
Renn, O. (2015) Ethikkommission: Wie legitim ist die Legitimation der Politik durch Wissenschaft? In P. Weingart and G.G. Wagner (eds), *Wissenschaftliche Politikberatung im Praxistest*. Weilerswist: Velbrück, 17–34.

Renn, O. (2016) Systemic risks: The new kid on the block. *Environment: Science and Policy for Sustainable Development*, 58(2), 26–36.

Renn, O. and Klinke, A. (2016) Complexity, uncertainty and ambiguity in inclusive risk governance. In T.J. Andersen (ed.), *The Routledge Companion to Strategic Risk Management*. New York and London: Routledge, 13–30.

Renn, O. and Levine, D. (1991) Credibility and trust in risk communication. In R.E. Kasperson and P.J.M. Stallen (eds), *Communicating Risks to the Public*. Dordrecht: Kluwer, 175–218.

Renn, O. and Walker, K. (2008) Lessons learned: A re-assessment of the IRGC framework on risk governance. In O. Renn and K. Walker (eds), *The IRGC Risk Governance Framework: Concepts and Practice*. New York: Springer, 331–67.

Righi, W.A., Saurin, T.A. and Wachs, P. (2015) A systematic literature review of resilience engineering: Research areas and a research agenda proposal. *Reliability Engineering and System Safety*, 141, 142–52.

Roache, P. (1998) *Verification and Validation in Computational Science and Engineering*. Albuquerque, NM: Hermosa Publishers.

Roberts, F.S. (1985) *Measurement Theory*. Cambridge: Cambridge University Press.

Rodrigues, M.A., Arezes, P. and Leão, S.P. (2014) Risk criteria in occupational environments: Critical overview and discussion. *Procedia – Social and Behavioral Sciences*, 109, 257–62.

Rohrmann, B. and Renn, O. (2000) Risk perception research: An introduction. In O. Renn and B. Rohrmann (eds), *Cross Cultural Risk Perception: A Survey of Empirical Studies*. Dordrecht: Kluwer, 11–54.

Rosa, E.A. (1998) Metatheoretical foundations for post-normal risk. *Journal of Risk Research*, 1, 15–44.

Rosa, E.A., Renn, O. and McCright, A.M. (2014) *The Risk Society Revisited. Social Theory and Governance*. Philadelphia: Temple University Press.

Rosness, R. and Forseth, U. (2014) Boxing and dancing: Tripartite collaboration as an integral part of a regulatory regime. In P. Lindøe, M. Baram and O. Renn (eds), *Risk Governance of Offshore Oil and Gas Operations*, 309–39. Cambridge, MA: Cambridge University Press.

Rosqvist, T. (2010) On the validation of risk analysis: A commentary. *Reliability Engineering and System Safety*, 95, 1261–5.

Rosqvist, T. and Tuominen, R. (2004a) Qualification of formal safety assessment: An exploratory study. *Safety Science*, 42, 99–120.

Rosqvist, T. and Tuominen, R. (2004b) Precautionary risk decision-making. *PSAM7 & ESREL'04 International Conference on Probabilistic Safety Assessment and Management, Berlin, 14-18 June 2004*. London: Springer-Verlag, 567–72.

Rowley, J. (2007) The wisdom hierarchy: Representations of the DIKW hierarchy. *Journal of Information Science*, 33(2), 163–80.

Rubin, G., Potts, H. and Michie, S. (2010) The impact of communications about swine flu (Influenza A H1N1v) on public responses to the outbreak: Results from 36 national telephone surveys in the UK. *Health Technology Assessment*, 14(34), 183–266.

Rutter, M. (1993) Resilience: Some conceptual considerations. *Journal of Adolescent Health*, 14(8), 626–31.

Sahlin, U. and Troffaes, M.C.M. (2017) A Note on EFSA's ongoing efforts to increase transparency of uncertainty in scientific opinions. *Journal of Risk Research*. DOI: 10.1080/13669877.2017.1313769.

Saltelli, A. and Funtowicz, S.O. (2017) What is science's crisis really about? *Futures*, 91, 5–11.
Sand, P. (2000) The precautionary principle: A European perspective. *Human and Ecological Risk Assessment*, 6(3), 445–58.
Sandin, P. (1999) Dimensions of the precautionary principle. *Human and Ecological Risk Assessment*, 5, 889–907.
Sandin, P., Peterson, M., Hansson, S.O., Rudén, C. and Juthe, A. (2002) Five charges against the precautionary principle. *Journal of Risk Research*, 5, 287–99.
Savage, L.J. (1954) *The Foundations of Statistics*. New York: John Wiley & Sons (2nd ed. 1972, New York: Dover).
Scheler, M. (1980) [1926]. *Problems of a Sociology of Knowledge*. London: Routledge.
SEP (2011) Stanford Encyclopedia Philosophy (Interpretations of probability). http://plato.stanford.edu/entries/probability-interpret/. Accessed July 2018.
Shapiro, A. (2013) On Kusuoka representation of law invariant risk measures. *Mathematics of Operations Research*, 38(1), 142–52.
Shewhart, W.A. (1931) *Economic Control of Quality of Manufactured Product*. New York: Van Nostrand.
Shewhart, W.A. (1939) *Statistical Method from the Viewpoint of Quality Control*. Washington, DC: Dover Publications.
Shortridge, J., Aven, T. and Guikema, S. (2017) Risk assessment under deep uncertainty: A methodological comparison. *Reliability Engineering and System Safety*, 159, 12–23.
Shrader-Frechette, K.S. (1984) Risk-cost benefit methodology and equal protection. In V.T. Covello, J. Menkes and J. Mumpower (eds), *Risk Evaluation and Management*. New York: Plenum Press, 275–96.
Siegrist, M., Keller, C. and Kiers, H.A.L. (2005) A new look at the psychometric paradigm of perception of hazards. *Risk Analysis*, 25(1), 211–22.
Sjöberg, L. (2000) Factors in risk perception. *Risk Analysis*, 220 (1), 1–11.
Sjöberg, L. (2003) Risk perception is not what it seems: The psychometric paradigm revisited. In K. Andersson (ed.), *VALDOR Conference 2003*. Stockholm: VALDOR, 14–29.
Sloman, S.A. (1996) The empirical case for two systems of reasoning. *Psychological Bulletin*, 119(1), 3–22.
Slovic, P. (1987) Perception of risk. *Science*, 236(4799), 280–5.
Slovic, P. (1992) Perception of risk: Reflections on the psychometric paradigm., In D. Golding and S. Krimsky (eds), *Theories of Risk*. Westport, CT: Praeger, 117–52.
Slovic, P., Finucane, M.L., Peters, E. and MacGregor, D.G. (2004) Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk and rationality. *Risk Analysis*, 24(2), 311–22.
Slovic, P., Finucane, M.L., Peters, E. and MacGregor, D.G. (2007) The affect heuristic. *European Journal of Operational Research*, 1777, 1333–52.
Smith, V.K. (1986) A conceptual overview of the foundations of benefit-cost analysis. In J.D. Bentkover, V.T. Covello and J. Mumpower (eds), *Benefits Assessment: The State of the Art*. Dordrecht: Reidel, 13–34.
Solberg, Ø. and Njå, O. (2012) Reflections on the ontological status of risk. *Journal of Risk Research*, 15(9), 1201–15.
Sower, V.E. (2014) *Essentials of Quality*. Hoboken, NJ: Wiley. .
SRA (2015a) Glossary Society for Risk Analysis, www.sra.org/resources. Accessed Jan. 2019.

SRA (2015b) Foundations of Risk Analysis. Discussion Note. http://sra.org/sites/default/files/pdf/FoundationsMay7-2015-sent-x.pdf. Accessed Jan. 2019.

SRA (2017a) Core Subjects of Risk Analysis, www.sra.org/resources. Accessed Jan. 2019.

SRA (2017b) Risk Analysis: Fundamental Principles, www.sra.org/resources. Accessed Jan. 2019.

Statoil ASA (2013) The In Amenas Attack. Report of the investigation into the terrorist attack on In Amenas. Prepared for Statoil ASA's board of directors. www.equinor.com/en/news/archive/2013/09/12/12SepInAmenasreport.html. Accessed Apr. 2019.

Stefánsson, O. (2019) On the limits of the precautionary principle. *Risk Analysis*.

Stern, P.C. and Fineberg, H.V. (1996) *Understanding Risk: Informing Decisions in a Democratic Society*. Washington, DC: US National Research Council.

Stirling, A. (1998) Risk at a turning point? *Journal of Risk Research*, 1, 97–109.

Stirling, A. (2007) Science, precaution and risk assessment: Towards more measured and constructive policy debate. *European Molecular Biology Organisation Reports*, 8, 309–15.

Sundstein, C.R. (2005) *Laws of Fear. Beyond the Precautionary Principle*. Cambridge: Cambridge University Press.

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

Taleb, N.N. (2012) *Anti Fragile*. London: Penguin.

Tamm Hallström, K. (2004) *Organizing International Standardization - ISO and the IASC in Quest of Authority*. Cheltenham: Edward Elgar.

Tamm Hallström, K. and Boström, M. (2011) *Transnational Multi-Stakeholder Standardization: Organizing a Fragile Non-State Authority*. Cheltenham: Edward Elgar.

Teng, K., Thekdi, S.A. and Lambert, J.H. (2012) Identification and evaluation of priorities in the business process of a risk or safety organization. *Reliability Engineering and System Safety*, 99, 74–86.

Teng, K., Thekdi, S.A. and Lambert, J.H. (2013) Risk and safety program performance evaluation and business process modeling. *IEEE Transactions on Systems, Man, and Cybernetics*: Part A, 42(6), 1504–13.

Thompson, K.M., Deisler Jr., P.H. and Schwing, R.C. (2005) Interdisciplinary vision: The first 25 years of the Society for Risk Analysis (SRA), 1980–2005. *Risk Analysis*, 25, 1333–86.

Tickner, J. and Kriebel, D. (2006) The role of science and precaution in environmental and public health policy. In E. Fisher, J. Jones, and R. von Schomberg (eds), *Implementing the Precautionary Principle*, 42–62. Northampton, MA: Edward Elgar Publishing.

Timmermans, S. and Epstein, S. (2010) A world of standards but not a standard world: Toward a sociology of standards and standardization. *Annual Review of Sociology*, 36, 69–89.

Trochim, W. (2000) *The Research Methods Knowledge Base*. 2nd ed. Cincinnati, OH: Atomic Dog Publishing.

Turner, B. and Pidgeon, N. (1997) *Man-made Disasters*. 2nd ed. London: Butterworth-Heinemann.

Tversky, A. and Kahneman, D. (1974) Judgment under uncertainty: Heuristics and biases. *Science*, 185(4157), 1124–31.

UK (2006) Guiding Principles of Governmental Risk Management. House of Lords. https://publications.parliament.uk/pa/ld200506/ldselect/ldeconaf/183/183i.pdf. Accessed July 2018.

UK (2018) Security Services M15 Threat Levels. https://www.mi5.gov.uk/threat-levels. Accessed Feb. 2017.

UNISDR (2015) Call for a Shift from Risk to Resilience. UN Secretary-General Ban Ki-moon https://www.unisdr.org/archive/46881. Accessed Feb. 2019.

Van Asselt, M.B.A. and Renn, O. (2011) Risk governance. *Journal of Risk Research*, 14(4), 431–49.

van der Sluijs, J., Craye, M., Futowicz, S., Kloprogge, P., Ravetz, J. and Risbey, J. (2005a) Combining quantitative and qualitative measures of uncertainty in model-based environmental assessment. *Risk Analysis*, 25(2), 481–92.

van der Sluijs, J., Craye, M., Funtowicz, S., Kloprogge, P., Ravetz, J. and Risbey, J. (2005b) Experiences with the NUSAP system for multidimensional uncertainty assessment in model based foresight studies. *Water Science and Technology*, 52(6), 133–44.

Vanem, E. (2012) Ethics and fundamental principles of risk acceptance criteria. *Safety Science*, 50, 958–67.

Veland, H. Amundrud, H. and Aven, T. (2013) Foundational issues in relation to national risk assessment methodologies. *Journal of Reliability and Risk*, 227, 348–58.

Veland, H. and Aven, T. (2013) Risk communication in the light of different risk perspectives. *Reliability Engineering and System Safety*, 110, 34–40.

Veland, H. and Aven, T. (2015) Improving the risk assessments of critical operations to better reflect uncertainties and the unforeseen. *Safety Science*, 79, 206–12.

Venkatasubramanian, V. (2011) Systemic failures: challenges and opportunities in risk management in complex systems. *AIChE Journal*, 57(1), 2–9.

Verhulsta, E. (2014) Applying systems and safety engineering principles for antifragility. *Procedia Computer Science*, 32, 842–9.

Viscusi, W.K., Hamilton, J.T. and Dockins, P.C. (1997) Conservative versus mean risk assessments: Implications for superfund policies. *Journal of Environmental Economics and Management*, 34, 187–206.

Visschers, V.H.M. (2018) Public perception of uncertainties within climate change science. *Risk Analysis*, 38(1), 43–55.

Visschers, V. H. M., Meertens, R.M., Passchier, W. W. F, and de Vries, N. N. K. (2009) Probability information in risk communication: A review of the research literature. *Risk Analysis*, 29, 267–87.

Vlek, C. (2011) Straightening out the grounds for precaution: A commentary and some suggestions about Terje Aven's "On Different Types of Uncertainties . . .". *Risk Analysis*, 31, 1534–7.

Vlek, C. (2013) How solid is the Dutch (and the British) national risk assessment? Overview and decision-theoretic evaluation. *Risk Analysis*, 33(6), 948–71.

Vose, D. (2008) *Risk Analysis: A Quantitative Guide*. 3rd ed. Chichester: Wiley.

Walliman. N. (2011) *Research Methods. The Basics*. London: Routledge.

Walls, J., O'Riordan, T., Horlick-Jones, T. and Niewöhner, J. (2005) The meta-governance of risk and new technologies: GM crops and mobile phones. *Journal of Risk Research*, 8(7–8), 635–61.

WBGU (2000) German Advisory Council on Global Change (Wissenschaftlicher Beirat der Bundesregierung Globale Umweltveränderungen). *World in Transition: Strategies for Managing Global Environmental Risk*. Heidelberg: Springer.

WEF (2018) *Global Risk Report*. Geneva: World Economic Forum.
Weich, K.E. and Sutcliffe, K.M. (2007) *Managing the Expected*. San Francisco, CA: Wiley.
Weinberg, A.M. (1981) Reflections on risk assessment. *Risk Analysis*, 1, 5–7.
WHO (2009) Current WHO phase of pandemic alert for Pandemic (H1N1) 2009. Geneva: World Health Organization. https://www.who.int/csr/disease/swineflu/phase/en/. Assessed Feb. 2019.
Wiegman, P.M., de Vries, H.J. and Blind, K. (2017) Multi-mode standardization: A critical review and a research agenda. *Research Policy*, 46, 1370–86.
Wiener, J.B and Rogers, M.D. (2002) Comparing precaution in the United States and Europe. *Journal of Risk Research*, 5(4), 317–49.
Wilson, R.S. and Arvai, J.L. (2006) When less is more: How affect influences preferences when comparing low and high-risk options. *Journal of Risk Research*, 9(2), 165–78.
Wolfs, F. (2009) Introduction to the Scientific Method. http://teacher.nsrl.rochester.edu/phy_labs/AppendixE/AppendixE.html. Accessed Nov. 2017.
Woods, D.D. (2015) Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering and System Safety*, 141, 5–9.
Wynne, B. (1992) Risk and social learning: Reification to engagement. In S. Krimsky and D. Golding (eds), *Social Theories of Risk*. Westport, CT: Praeger, 275–97.
Xiong, Y., Chen, W., Tsui, K.L. and Apley, D.W. (2009) A better understanding of model updating strategies in validating engineering models. *Journal of Computer Methods in Applied Mechanics and Engineering*, 198(5), 1327–37.
Yadav, M. (2010) The decline of conceptual articles and implications for knowledge development. *Journal of Marketing*, 74 (Jan.), 1.
Yamaguchi, N., Kobayashi, Y.M. and Utsunomiya, O. (2000) Quantitative relationship between cumulative cigarette consumption and lung cancer mortality in Japan. *International Journal of Epidemiology*, 29(6), 963–8.
Zajonc, R.B. (1980) Feeling and thinking: Preferences need no inferences. American Psychologist, 35, 151–75.
Zimmennann, R. (1987) A process framework for risk communication. *Science, Technology, and Human Values*, 12 (Summer/Fall), 131–7.
Zins, C. (2007) Conceptual approaches for defining data, information, and knowledge. *Journal of the American Society for Information Science and Technology*, 58(4), 479–93.
Zio, E. (2006) A study of the bootstrap method for estimating the accuracy of artificial neural networks in predicting nuclear transient processes. *IEEE Transactions on Nuclear Science*, 53(3), 1460–78.
Zio, E. (2009) Reliability engineering: Old problems and new challenges. *Reliability Engineering and System Safety*, 94, 125–41.
Zio, E. (2016) Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering and System Safety*, 152, 137–50.
Zio, E. (2018) The future of risk assessment. *Reliability Engineering and System Safety*, 177, 176–90.
Zio, E. and Apostolakis G.E. (1996) Two methods for the structured assessment of model uncertainty by experts in performance assessments of radioactive waste repositories. *Reliability Engineering and System Safety*, 54, 225–41.

Index

Page numbers for figures are given in *italics*, and for tables they are given in **bold.**