MARVIN RAUSAND

Risk Assessment

Theory, Methods, and Applications

STATISTICS IN PRACTICE

WILEY

WWW. LINK AVAILABLE

RISK ASSESSMENT

STATISTICS IN PRACTICE

Advisory Editor

Wolfgang Jank
University of Maryland, USA

Founding Editor

Vic Barnett
Nottingham Trent University, UK

The texts in the series provide detailed coverage of statistical concepts, methods, and worked case studies in specific fields of investigation and study.

With sound motivation and many worked practical examples, the books show in down-to-earth terms how to select and use an appropriate range of statistical techniques in a particular practical field. Readers are assumed to have a basic understanding of introductory statistics, enabling the authors to concentrate on those techniques of most importance in the discipline under discussion.

The books meet the need for statistical support required by professionals and research workers across a range of employment fields and research environments. Subject areas covered include medicine and pharmaceutics; industry, finance, and commerce; public services; the earth and environmental sciences.

A complete list of titles in this series appears at the end of the volume.

RISK ASSESSMENT

Theory, Methods, and Applications

MARVIN RAUSAND
Norwegian University of Science and Technology

A JOHN WILEY & SONS, INC., PUBLICATION

Cover photo credit: Helge Hansen/Statoil

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:

Rausand, Marvin.
Risk assessment : theory, methods, and applications / Marvin Rausand.
p. cm. — (Statistics in practice)
Includes index.
ISBN 978-0-470-63764-7 (hardback) *
1 Technology—Risk assessment. 2. Risk assessment. I. Title.
T174.5.R37 2011
363.1'02—dc22 2011010971

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

To Hella, Guro, and Idunn

CONTENTS

Preface

This book gives a comprehensive introduction to risk analysis and risk assessment, and the main methods for such analyses. It deals with accidents that may occur in technical or sociotechnical systems with focus on sudden, major accidents. Day-to-day occupational accidents and negative health effects due to long-term exposure are therefore outside the scope of the book.

In 1991, the Norwegian standard NS 5814, *Requirements to Risk Analysis*, was issued and I wrote a small book in Norwegian called *Risk Analysis: Guidance to NS 5814* (Rausand, 1991). The book was very basic but filled a purpose and was used extensively. I began to write the current book in 1995 after the first edition of the book *System Reliability Theory* was published. After awhile I realized that writing a book on risk assessment was much more difficult than writing a book on system reliability. This was due mainly to the confusing terminology, the multidisciplinary character of the topics, and the overwhelming number of reports and guidelines that had been written.

In 2008, the second edition of NS 5814 was issued and the guideline had to be updated and extended. This resulted in the book *Risk Analysis: Theory and Methods* (Rausand and Utne, 2009b), which is written in Norwegian and coauthored by Ingrid Bouwer Utne. The book was strongly influenced by the manuscript of the current book, has a similar structure, but is more basic and straightforward.

The current book is divided into two main parts. Part I introduces risk analysis and defines and discusses the main concepts used. Our understanding of how accidents occur will always influence our approach to risk assessments, so a chapter describing accident models and accident causation is therefore included. Input data requirements and data quality are also presented in a separate chapter. The various steps of a risk assessment are explained and arranged in a structure.

Part II deals with the main methods of risk analysis, such as preliminary hazard analysis, HAZOP, fault tree analysis, and event tree analysis. Special problem areas such as common-cause failures and human errors are also discussed. Part II ends with a brief survey of the development and application of risk assessment in some main application areas.

Part III of the book contains appendices. Some main results from probability and statistics are given in Appendix A. Readers who have not taken a basic course in probability and statistics should consider reading this appendix first. Other readers may find it useful to check formulas in the appendix. Part III also contains a list of acronyms and a glossary of main terms used in risk assessment.

The book gives several references to laws, regulations, and standards. When using these references, you should always check to see if new versions have been made available.

Several organizations have issued a number of technical reports and guidelines related to risk assessment. Many of these are of very high quality but often use conflicting terminology, and they present a multitude of methods with more or less the same purpose. Very few textbooks on risk assessment are on the market, however.

To contribute to a more standardized terminology in risk assessment, I have put considerable effort into using a stringent terminology and giving clear definitions. The main definitions are written as separate paragraphs preceded by the symbol ☞.

When writing this book, I have read guidelines from many different organizations and tried to extract the main messages from these guidelines. Such guidelines seem to be issued faster than I am able to read, so I cannot claim that I cover all of them. There are certainly several important organizations that I have missed while searching for guidelines. Among these are obviously guidelines that are written in languages that I am not able to understand.

I have selected methods that are commonly applied and that I find useful. Whether or not this is a good selection is up to you to judge. The book may perhaps be accused of being old-fashioned because I have included mainly proven methods instead of brand-new suggestions.

Within some areas of risk assessment, such as human reliability analysis, there are a vast number of approaches, and it seems to be a strategy that every person working with human reliability should develop her/his own method.

Suggestions for further reading are provided at the end of each chapter. I do not claim that the references listed are the most relevant that can be found. Rather, these are the references I have found most useful and that are most in line with the views presented in this book.

The book is written mainly as a textbook for university courses in risk analysis and risk assessment. For this reason, a set of problems have been developed and are available on the book's homepage, `http://www.ntnu.edu/ross/books/risk`.

The book is also intended to be a guide for practical risk assessments. The various methods are therefore described sufficiently that you should be able to use the method after having read the description. Each method is described according to the same structure, and the various steps of the methods are listed and often also illustrated in workflow diagrams. The descriptions of the methods are, as far as possible, self-contained, and it should therefore not be necessary to read the entire book to have enough background to use the individual methods.

The descriptions and examples given in the book are largely from Europe, especially from Norway. I trust, however, that most of the book is also relevant in other parts of the world.

The book is written in a style similar to that used in my book on system reliability theory (Rausand and Høyland, 2004). Some methods are treated in both books, but from different standpoints. Several issues are described in more detail in Rausand and Høyland (2004), and I therefore recommend that you have both books available, even if it is not strictly required.

I hope that you will enjoy reading this book and that you will find it useful. If you have questions or comments, you will find my email address on the book's homepage (see below).

M. RAUSAND

Trondheim, Norway
March 15, 2011

For more information, see `http://www.ntnu.edu/ross/books/risk`.

Acknowledgments

It is a pleasure to acknowledge and thank several friends and colleagues whose ideas and suggestions have contributed greatly to the book. I mention them in alphabetical order.

- Stein Haugen is a professor in risk analysis at NTNU and has extensive experience using risk analyses in industry projects. He has read several chapters and given many helpful comments that have improved the book.

- Per Hokstad of SINTEF coauthored an earlier version of Chapter 15 on common-cause failures and has strongly influenced the content of that chapter.

- Inger Lise Johansen is a Ph.D. student at NTNU. I have the pleasure of being the supervisor of her master's thesis and currently of her Ph.D. project. Her master's thesis was written in parallel with Chapters 2 and 4 of this book, and she has made significant contributions to these chapters. She has also read several other chapters, reformulated some of my clumsy expressions, added content, and made valuable comments as to both language and content.

- Ondřej Nývlt of the Czech Technical University in Prague spent six months at NTNU as an exchange Ph.D. student. I had the pleasure of being his local supervisor, and he helped me to write the section on Petri nets in Chapter 10.

- Ingrid Bouwer Utne coauthored the Norwegian book *Risk Analysis; Theory and Methods* (Rausand and Utne, 2009a) while she was a postdoc at NTNU. Our discussions and her ideas have also clearly influenced the current book.

- Knut Øien of SINTEF is also an adjunct professor in risk assessment at NTNU. He coauthored an early draft of Chapter 13 on human reliability analysis and has read and commented on the final version. Chapter 17, describing the development and application of risk assessment, is based on a note in Norwegian that Knut Øien and I wrote some years ago.

I also acknowledge the editing and production staff at John Wiley & Sons for their careful, effective, and professional work.

I thank the International Electrotechnical Commission (IEC) for permission to reproduce information from the standards IEC 60300-3-9 ed.1.0 (1995), IEC 60300-3-4 ed.2.0 (2007), IEC 60050-191 ed.1.0 (1990), IEC 61508-0 ed. 1.0 (2005), IEC 61508-4 ed.2.0 (2010), IEC 61508-1 ed.2.0 (2010), IEC 61508-6 ed.2.0 (2010). All such extracts are copyright of IEC, Geneva, Switzerland. ©All rights reserved. Further information on the IEC is available from `http://www.iec.ch`. IEC has no responsibility for the placement and context in which the extracts and contents are reproduced by the author, nor is IEC in any way responsible for the other content or accuracy herein.

Point 2.13 from NS-ISO 31000:2009 Risk management - Principles and guidelines, as well as definitions in 2.1.1, 2.1.5, 2.1.13, 2.1.20 and Table A.1 from NS-EN ISO 17776:2002 are reproduced in this book under license from Standard Online AS 03/2011. ©All rights reserved. Standard Online makes no guarantees or warranties as to the correctness of the reproduction.

Several references are given to publications by the UK Health and Safety Executive (HSE). This is public sector information published by the HSE and licensed under the Open Government Licence v.1.0.

The book was completed during my sabbatical year at ParisTech, Ecole Nationale Supérieure d'Arts et Métiers (ENSAM) in Aix en Provence, France. I am very grateful to Professor Lionel Roucoules and his colleagues, who helped me and made this stay a positive experience.

During the writing of the book, I have read many books, scientific articles, standards, technical reports, guidelines, and notes related to risk assessment. I have tried to process, combine, and reformulate the information obtained and I have tried to give proper references. If I unconsciously copied sentences without giving proper reference, it has not been my intention, and I apologize if that has happened.

In the preface of the book *The Importance of Living* (William Morrow, New York, 1937), Lin Yutang writes: "I must therefore conclude by saying as usual that the merits of this book, if any, are largely due to the helpful suggestions of my collaborators, while for the inaccuracies, deficiencies and immaturities of judgment, I alone am responsible." If the word *collaborators* is replaced by *colleagues and references*, this statement applies equally well for the current book.

M.R.

PART I

INTRODUCTION TO RISK ASSESSMENT

CHAPTER 1

INTRODUCTION

> Risk is a curious and complex concept. In a sense it is unreal in that it is always concerned with the future, with possibilities, with what has not yet happened.
>
> —Elms (1992)

1.1 INTRODUCTION

If you ask ten people what they mean by the word *risk*, you will most likely get ten different answers. The same inconsistency also prevails in newspapers and other media. A brief search for the word *risk* in some Internet newspapers gave the results in Table 1.1. In some of the statements, the word *risk* can be replaced with *chance*, *likelihood*, or *possibility*. In other cases, it may be synonymous with *hazard*, *threat*, or *danger*. The situation is not much better in the scientific community, where the interpretation is almost as varying as among the general public. A brief search in risk assessment textbooks, journal articles, standards, and guidelines will easily prove that this applies also for the specialists in risk assessment.

In 1996, the prominent risk researcher Stan Kaplan received the Distinguished Award from the Society of Risk Analysis. To express his gratitude, Kaplan gave a

Risk Assessment: Theory, Methods, and Applications, First Edition. Marvin Rausand.

Table 1.1 The word *risk* as used in some Internet newspapers (in May 2010).

...the government would risk a humiliating defeat ...	...because of the risk of theft ...
...people judged to be at high risk of having a fall ...	...the number of homes exposed to flood risk could increase ...
...there's no simple equation for predicting divorce risk ...	...a more environmentally risky mode of getting our energy ...
...investors are willing to take on a high risk ...	...risk appetite for equities and corporate bonds...
...encouraged financiers to seek out greater profits by taking risks in areas beyond regulatory purview...	...by reducing the risk of collisions with vehicles ...
...the flight from risk has hit the stock markets ...	...bicycle helmets have been shown to reduce the risk of head injuries by up to 88 percent ...
...investments that had put their capital at risk ...	...a high-risk attempt to plug the leaking oil well ...
...we could put at risk our food and water supplies ...	...carries an accident risk of "Chernobyl proportions" ...
...she was considered at risk because of her work ...	...that created the illusion that risk was being responsibly managed ...

talk to the plenary session at the society's annual meeting. In the introduction to this talk, he said: [1]

> The words of risk analysis have been, and continue to be a problem. Many of you remember that when our Society for Risk Analysis was brand new, one of the first things it did was to establish a committee to define the word "risk." This committee labored for 4 years and then gave up, saying in its final report, that maybe it's better not to define risk. Let each author define it in his own way, only please each should explain clearly what way that is (Kaplan, 1997).

1.1.1 Three Main Questions

Risk (as used in this book) is always related to what can happen in the future. In contrast to our ancestors, who believed that the future was determined solely by the acts of God (e.g., see Bernstein, 1996), we have the conviction that we can analyze and manage risk in a rational way. Our tool is *risk analysis*, and the goal is to inform decision-making concerning our future welfare.

[1] Reprinted from Risk Analysis, Vol. 17, Kaplan, S. "The words of risk analysis", Copyright (1997), with permission from Wiley-Blackwell.

The possibility of harmful events is an inherent part of life. Such events can be caused by natural forces, such as flooding, earthquake, or lightning; technical failures; or human actions. Some harmful events can be foreseen and readily addressed, while others come unexpectedly because they appear unforeseeable or have only a very remote likelihood of occurrence. In many systems, various safeguards are installed to prevent harmful events or to mitigate the consequences should such events occur. Risk analysis is used to identify the causes of harmful events, to determine the possible consequences of harmful events, to identify and prioritize barriers, and to form a basis for deciding whether or not the risk related to a system is *tolerable*.

A risk analysis is carried out to provide answers to the following three main questions (Kaplan and Garrick, 1981):

Q1. *What can go wrong?*
To answer this question, we must identify the possible *hazardous events*[2] that may lead to *harm* to some *assets* that we want to keep and protect. These assets may be people, animals, the environment, buildings, technical installations, infrastructure, cultural heritage, our reputation, information, data, and many more.

Q2. *What is the likelihood of that happening?*
The answer can be given as a qualitative statement or as probabilities or frequencies. We consider the hazardous events that were identified in Q1, one by one. To determine their likelihood, we often have to carry out a causal analysis to identify the basic causes (*hazards* or *threats*) that may lead to the hazardous event.

Q3. *What are the consequences?*
For each hazardous event, we must identify the potential harm or adverse *consequences* to the assets mentioned in Q1. Most systems have *barriers* that are installed to prevent or mitigate harm. The harm to the assets is dependent on whether or not these barriers function when the hazardous event takes place.

For now, we suffice by defining risk as the answer to these three questions.

1.1.2 A Conceptual Model

For each hazardous event that is identified by answering Q1, the analytical process used to answer Q2 and Q3 may be illustrated by Figure 1.1. The figure illustrates that various hazards and/or threats may lead to a hazardous event, and that the hazardous event may in turn lead to many different consequences. Various barriers are often available between the hazards/threats and the hazardous event, and also between the hazardous event and the consequences. The model in Figure 1.1 is called a *bow-tie model* because it resembles the bow-tie that men sometimes use in place of a necktie with a formal suit.

[2]Kaplan and Garrick (1981) use the term *scenario* instead of *hazardous event*.

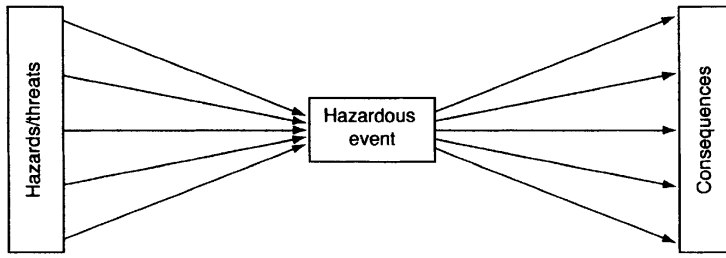

Figure 1.1 A simpli ed bow-tie model.

The bow-tie model is useful for illustrating both the conception and analysis of risk. The terms needed to answer the three related questions of Kaplan and Garrick (1981) have, however, been interpreted differently by various sources and practitioners, as have the methods in which they are used. Today, numerous laws and regulations require that risk analyses or risk assessments be carried out, but there is still no unified terminology or standard framework for carrying out these assessments.

1.1.3 Objective of the Book

The main objective of this book is to give a comprehensive introduction to risk assessment and present the essential theory and the main methods that can be used to perform a risk assessment of a technical or sociotechnical system.

More specific objectives are:

(a) To present and discuss the terminology used in risk assessment of technical and sociotechnical systems. A vague hope is that this may contribute to a more harmonized terminology in risk assessment.

(b) To define and discuss how risk can be quantified and how these metrics may be used to evaluate the tolerability of risk.

(c) To present the main methods for risk assessment and discuss the applicability, advantages, and limitations of each method.

(d) To present and discuss some main problem areas related to risk assessment (e.g., human errors, dependent failures).

(e) To describe how a risk assessment may be carried out in practice and illustrate some important application areas.

1.1.4 Focus of the Book

This book is mainly concerned with risk related to:

- a technical or sociotechnical *system* in which

- *events* may occur in the *future* and that
- have *unwanted consequences*
- to *assets* that we want to protect.

The systems to be considered may be any type of engineered system, ranging from small machines up to complex process plants or transportation networks. This book does not cover all aspects of risk, but is limited to *accidents* where an abrupt event may give negative outcomes (some kind of loss or damage). Adverse effects caused by continuous and long-term exposure to a hazardous environment or dangerous materials (e.g., asbestos) are thus not covered unless the exposure is caused by a specific event (e.g., an explosion). Neither is an objective of this book to present and discuss detailed physical consequence models, such as fire and explosion models.

In the financial world, investments are often made and risk is taken to obtain some benefit. The outcome may be either positive or negative, and risk is then a statement about the *uncertainty* regarding the outcome of the investment. This interpretation of the word *risk* is not relevant for this book, which is concerned exclusively with adverse outcomes.

The main focus of the book is risk assessment *per se*, not how the results from the assessment may be used or misused. Some issues related to risk *management* are, however, discussed briefly in Chapter 5.

The objective of this introductory chapter is to introduce the main concepts used in risk assessment and to place risk assessment into a decision-making context.

1.2 RISK ANALYSIS, ASSESSMENT, AND MANAGEMENT

1.2.1 Risk Analysis

So far, we have mentioned risk analysis several times, but not given any clear definition. A commonly used definition is:

☞ **Risk analysis**: Systematic use of available information to identify hazards and to estimate the risk to individuals, property, and the environment (IEC 60300-3-9, 1995).

A risk analysis is always a *proactive* approach in the sense that it deals exclusively with potential accidents. This is opposed to accident investigation, which is a *reactive* approach that seeks to determine the causes and circumstances of accidents that have already happened.

Three Main Steps. As indicated in Section 1.1, a risk analysis is carried out in three main steps by providing answers to the three questions in Section 1.1.2:

1. *Hazard identification.* In this step, the hazards and threats related to the system are identified together with the potential hazardous events. As part of this process, assets that may be harmed are also identified.

2. *Frequency analysis.* This step will usually involve a deductive analysis to identify the causes of each hazardous event and to estimate the frequency of the hazardous event based on experience data and/or expert judgments.

3. *Consequence analysis.* Here, an inductive analysis is carried out to identify all potential sequences of events that can emerge from the hazardous event. The objective of the inductive analysis is usually to identify all potential end consequences and also their probability of occurrence.

Qualitative vs. Quantitative Analysis. The risk analysis may be qualitative or quantitative, depending on the objective of the analysis.

☞ **Qualitative risk analysis**: A risk analysis where probabilities and consequences are determined purely qualitatively.

☞ **Quantitative risk analysis (QRA)**: A risk analysis that provides numerical estimates for probabilities and/or consequences—sometimes along with associated uncertainties.

A QRA is best suited for quantifying risk associated with low-probability and high-consequence events, and may range from specialized probabilistic assessment to large-scale analysis. The term *semiquantitative risk analysis* is sometimes used to denote risk analyses that quantify probabilities and consequences approximately within ranges.

Remark: Some industries use other names for the QRA. In the U.S. nuclear industry and in the space industry, the QRA is called *probabilistic risk analysis* (PRA). In the European nuclear industry, QRA is referred to as *probabilistic safety analysis* (PSA), whereas the maritime industry uses the term *formal safety assessment* (FSA). The term *total risk analysis* (TRA) sometimes appears in the Norwegian offshore industry. ⊕

Types of Risk Analyses. Risk analyses can be classified in many different ways. One attempt of classification can be made on the basis of Figure 1.2, which displays three categories of hazards and and three categories of assets in a 3×3 matrix.

This book is concerned mainly with the last column of Figure 1.2, where the hazard source is a technical system or some dangerous materials. The other types of risk analyses are, however, also discussed briefly.

1.2.2 Risk Evaluation

We distinguish between risk analysis and *risk evaluation*, which may be defined as:

☞ **Risk evaluation**: Process in which judgments are made on the tolerability of the risk on the basis of a risk analysis and taking into account factors such as socioeco-

Assets	Hazard source		
	Humans	The environment	Technology / materials
Humans	1	2	3
The environment	4	5	6
Material / financial	7	8	9

Figure 1.2 Different types of risk analyses.

nomic and environmental aspects (IEC 60300-3-9, 1995).

The risk evaluation will sometimes include a comparison of the results from the risk analysis with some *risk acceptance criteria*. Risk acceptance criteria are discussed further in Chapter 4.

Too often, it happens that the management does the risk evaluation without any involvement from those who have produced the risk analysis. This may create communication problems and lead to erroneous inferences, and it is therefore strongly recommended that the risk analysts also be involved in the evaluation.

1.2.3 Risk Assessment

When risk analysis and risk evaluation are carried out in a joint process, we say that we do a *risk assessment*.

☞ **Risk assessment**: Overall process of risk analysis and risk evaluation (IEC 60300-3-9, 1995).

■ **EXAMPLE 1.1 Five steps to risk assessment**

The UK HSE has published a simple and informative introduction to risk assessment called *Five steps to risk assessment* (HSE, 2006). The five steps are:

1. Identify the hazards.
2. Decide who might be harmed and how.
3. Evaluate the risks and decide on precautions.
4. Record your findings and implement them.
5. Review your assessment and update if necessary. ⊕

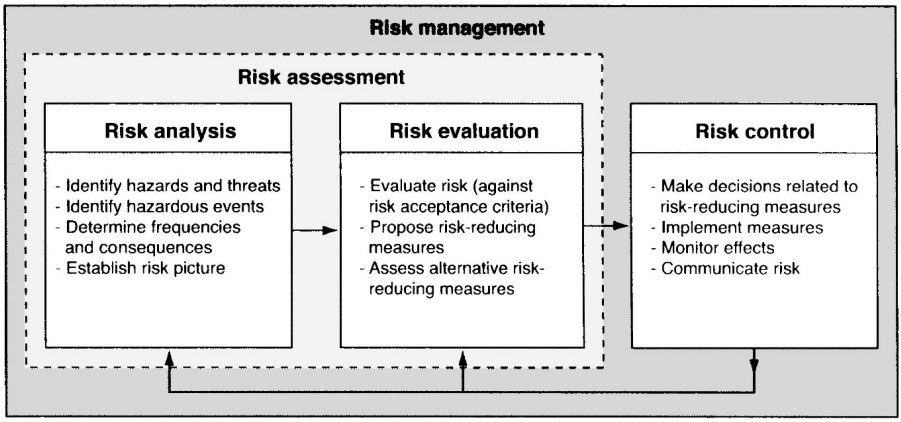

Figure 1.3 Risk analysis, evaluation, assessment, and management (see also IEC 60300-3-9, 1995).

Remark: Some books and guidelines do not distinguish between risk analysis and risk assessment and tend to use the term *risk assessment* also when risk evaluation is not part of the job. Other guidelines define risk assessment as an add-on to risk evaluation. An example here is the U.S. Federal Aviation Administration, which defines risk assessment as "the process by which the results of risk analysis are used to make decisions" (US FAA, 2000, App. A). ⊕

1.2.4 Risk Management

If we, in addition, identify and (if necessary) implement risk-reducing actions and survey how the risk changes over time, we conduct *risk management*.

☞ **Risk management**: A continuous management process with the objective to identify, analyze, and assess potential hazards in a system or related to an activity, and to identify and introduce risk control measures to eliminate or reduce potential harms to people, the environment, or other assets.

Slightly different definitions of risk management may be found in guidelines and textbooks. Some of these stress that risk management is a proactive and systematic approach to setting the best course of action under uncertainty, and that it also involves communicating the risk to the various stakeholders (e.g., see Treasury Board, 2001).

Although this book is focused primarily on risk analysis, we also present some views on risk evaluation and risk management. The elements of risk management are illustrated in Figure 1.3 and are discussed further in Chapter 5.