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*.

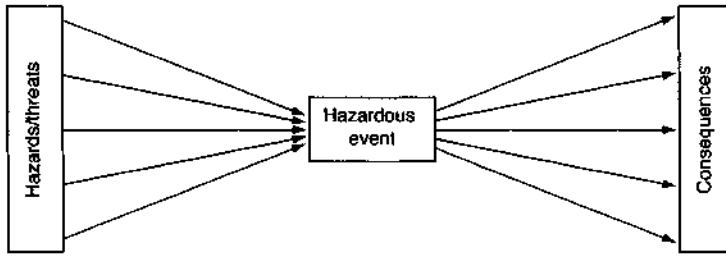

Figure 1.1 A simpli ed bow-tie model.

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. ⊕

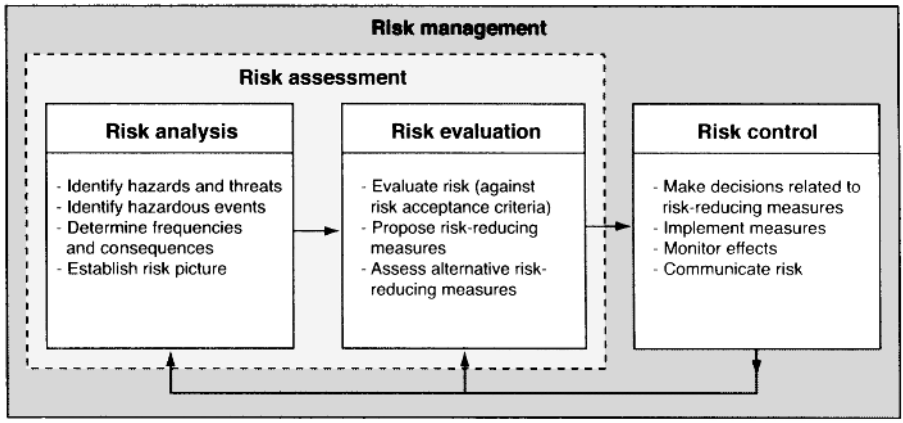

Figure 1.3 Risk analysis, evaluation, assessment, and management (see also IEC 60300-3-9, 1995).

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.

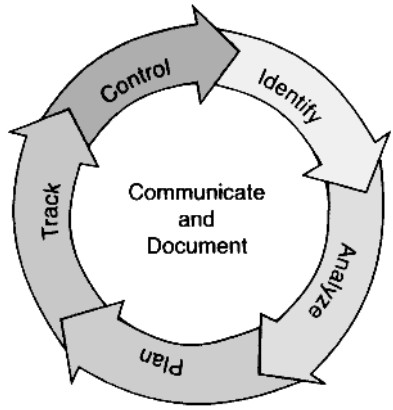

Figure 1.4 Continuous risk management process (based on NASA, 2008).

Continuous Risk Management. Risk management is a continuous management process, which often contains the following six elements as illustrated in Figure 1.4 (e.g., see NASA, 2008)[3]:

Identify. Before the risk can be managed, the hazards and the potential hazardous events must be identified. The identification process may reveal problems before they come to the surface. The problems should be stated, describing what, when, where, how, and why the hazardous event might happen.

Analyze. Analysis means in this regard to convert data related to risk into decision-relevant information. The data may be related to the likelihood of a hazardous event and the severity of harm if the event should happen. The analysis provides the basis from which the company can prioritize the most critical risk elements.

Plan. Here, the risk information is turned into decisions and actions. Planning involves developing actions to address individual hazards, prioritizing risk-reducing actions, and creating an integrated risk management plan. The key to risk action planning is to consider the future consequences of a decision made today.

Track. Tracking consists of monitoring the risk level and the actions taken to reduce the risk. Appropriate risk metrics are identified and monitored to enable the evaluation of the status of risk.

Control. Here, proposed risk-reducing actions are executed and controlled. The step is integrated into general management and relies on management processes to con-

[3]A similar figure may also be found in the following: Strategy Unit (2002, p. 44) and Treasury Board (2001, p. 26).

trol risk action plans, correct deviations from plans, respond to events, and improve risk management processes.

Communicate and Document. The activities described above should be documented and communicated. Risk communication is placed at the center of the model to emphasize both its pervasiveness and its criticality. Without effective communication, no risk management approach can be viable. A system for documentation and tracking of risk decisions must be implemented.

1.3 THE STUDY OBJECT

In this book, the object of analysis is a technical or sociotechnical system. We refer to this as the *study object* or the *system*. A system may be defined as:

☞ **System**: Composite entity, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task to achieve a specific objective (IEC 60300-3-9, 1995).

When analyzing a study object, it is always wise to remember the influential risk researcher Jens Rasmussen's statement that "a system is more than the sum of its elements" (Rasmussen, 1997).

1.3.1 The Sociotechnical System

If people have important roles or relations to and within a system, we often refer to the study object as a *sociotechnical system*. A sociotechnical system will contain several types of elements, such as:

- *Hardware* (H). Any physical and nonhuman element of the study object, such as workspace, buildings, machines, equipment, and signs.
- *Software* (S). Nonmaterial elements of the study object: for example, computer software, work procedures, norms, checklists, and practices.
- *Liveware* (L). Personnel, such as operators, maintenance staff, service personnel, visitors and third parties. Liveware also includes such elements as teamwork and leadership.
- *Management/organization* (M). Management, policies, strategies, training, and so on.
- *Environment* (E). The internal and external environment in which the study object operates.

The various elements of the study object are illustrated in Figure 1.5. In a risk analysis, it is important to consider all these elements and the interfaces between them.

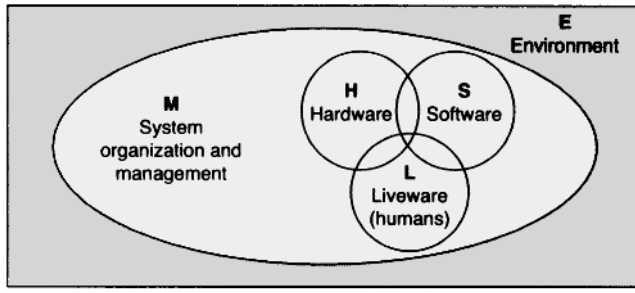

Figure 1.5 The elements of a study object (see also IEC 60300-3-4, 2007).

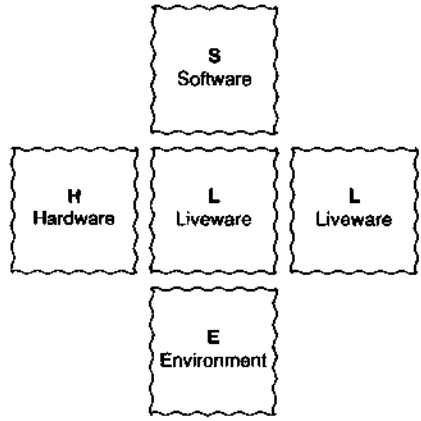

Figure 1.6 SHEL model.

Most study objects will also have interfaces with other objects that have to be considered in the risk analysis. To make sure that all relevant interfaces are considered, the aviation industry advocates the SHEL model.

1.3.2 The SHEL Model

The SHEL model was developed within the aviation industry through the 1970s and early 1980s. The name of the model is derived from the initial letters of its four elements: software (S), hardware (H), environment (E), and liveware (L).

The SHEL model is illustrated in Figure 1.6, where the boxes are drawn with rugged lines to emphasize the often complicated interfaces between the elements. In a risk analysis, all possible interfaces should be studied. Important interfaces are (e.g., see ICAO, 2009):

(a) *Liveware-Hardware (L-H).* This interface between the human and the hardware is often called the *man-machine interface*.

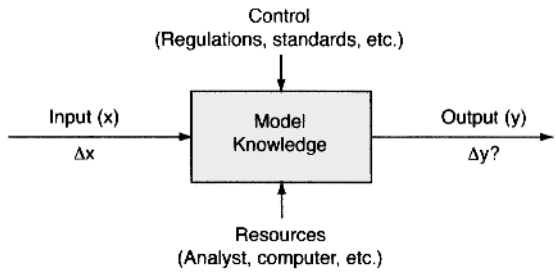

Figure 1.7 System inputs and outputs.

(b) *Liveware-Software (L-S).* This interface describes the relationship between the personnel and the computer software, checklists, and so on. It depends on the presentation format, clarity, and the use of symbols.

(c) *Liveware-Liveware (L-L).* This interface covers the relationship between the individual and other persons in the workplace. It depends on leadership, cooperation, teamwork, and personal interactions.

(d) *Liveware-Environment (L-E).* This interface concerns the relationship between the individual and her/his internal and external environments. The internal environment involves factors such as temperature, light, noise, vibration, and air quality. The external environment includes such things as weather conditions and external systems that may influence the working conditions.

1.3.3 Complexity and Coupling

When analyzing the relationships between the elements in a sociotechnical system, risk assessment is riddled by two main challenges: complexity and coupling. These concepts were actualized in Charles Perrow's seminal book *Normal Accidents: Living with High-Risk Technologies* (Perrow, 1984) and are discussed further in Chapter 6.

Complexity. The input and output of a system or a system element are illustrated in Figure 1.7. The input x (which may be a vector) will produce an output y (which may also be a vector). If a change Δx is made to the input, knowledge and models may be used to predict the change Δy of the output. The complexity of the system is characterized by our ability to predict the change Δy of the output caused by a specified change Δx of the input. If we, without any uncertainty, can predict the change Δy, the system is said to be *linear*. In the opposite case, the system is said to be *complex*. The degree of complexity increases with the uncertainty about the value of Δy. The extreme case is when we do not have any clue about what will happen to y when we change the input x.

Complexity leads to several challenges in a risk analysis, as pinpointed by Leveson (1995):

Table 1.2 Characteristics of tight and loose coupling systems.

Tight coupling	Loose coupling
Delays in processing not possible	Processing delays are possible
Order of sequences cannot be changed	Order of sequence can be changed
Only one method is applicable to achieve the goal	Alternative methods are available
Little slack possible in supplies, equipment, personnel	Slack in resources possible
Buffers and redundancies may be available, but are deliberately designed-in, and there is no flexibility	Buffers and redundancies fortuitously available
Substitutions of supplies, equipment, and personnel may be available, but are limited and designed-in	Substitutions are fortuitously available

Source: Adapted from Perrow (1984), also cited by Stewart and Melchers (1997).

> Many of the new hazards are related to increased complexity (both product and process) in the systems we are building. Not only are new hazards created by the complexity, but the complexity makes identifying them more difficult.

The ever-increasing integration of information and communication technology in systems and the expanding digital infrastructure are important contributors to system complexity. This problem is discussed further by Grøtan et al. (2011).

Coupling. The other important concept discussed by Perrow (1984) is *coupling*, which may be defined as a measure of the strength of the interconnectedness between system components. Perrow (1984) is concerned mainly with *tight coupling*:

> The sub-components of a tightly coupled system have prompt and major impacts on each other. If what happens in one part has little impact on another part, or if everything happens slowly (in particular, slowly on the scale of human thinking times), the system is not described as *tightly coupled*. Tight coupling also raises the odds that operator intervention will make things worse, since the true nature of the problem may well not be understood correctly.

Some of the main characteristics of tight and loose coupling are listed in Table 1.2.

1.4 ACCIDENT CATEGORIES

When analyzing risk, the most suitable approach will vary with the type of accidents we are faced with. Different types of accidents may be distinguished by their frequency, origin, and/or impact.

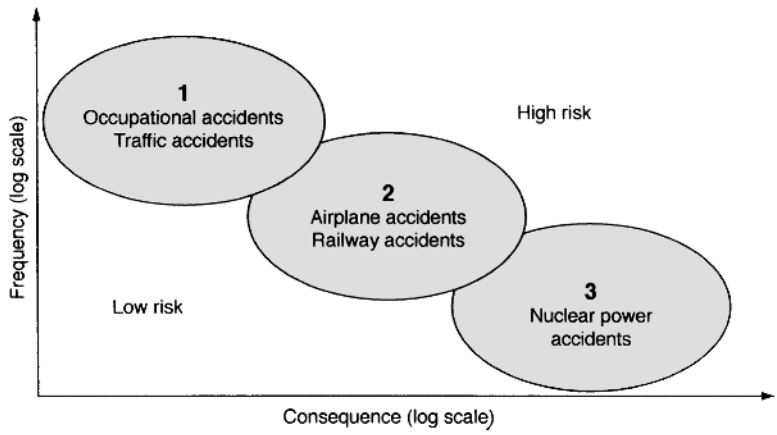

Figure 1.8 Three main categories of accidents (adapted from Rasmussen, 1997).

1.4.1 Jens Rasmussen's Categories

Accidents can, according to Rasmussen (1997), be classified into three main categories, as illustrated in Figure 1.8.

Accidents of Category 1. Some accidents, such as road traffic accidents and minor occupational accidents, occur so often and so "regularly" that we may predict the number of similar accidents in the near future based on past observations. Accidents of this category are characterized by a relatively high frequency and a correspondingly low consequence.

Accidents of Category 2. Accidents of category 2 in Figure 1.8 occur rather seldom and have more severe consequences than the accidents in category 1. Examples of such accidents are major industrial accidents, air accidents, railway accidents, and maritime accidents. In the aftermath of such accidents, detailed accident investigations are usually carried out to identify the possible causes of the accident and what could have been done to prevent it from occurring. To determine the risk related to such accidents, it is not sufficient to base the assessment on the number of accidents observed in the past. Rather, we should carry out a detailed risk analysis to identify all the possible hazards and accident scenarios that have yet to occur. Each part of the system is then analyzed and the total risk is determined based on the risk related to the various parts.

Accidents of Category 3. Accidents of category 3 in Figure 1.8 occur very seldom, but when they do, they have catastrophic and wide-ranging consequences. An example of an accident in this category is the Chernobyl nuclear power accident in 1986. For such accidents, it has no meaning whatsoever to try to determine the risk based on historical data. It is therefore necessary to carry out detailed risk analyses of the various parts of the system.

The risk analyses that are covered in this book are mainly relevant for systems that produce accidents in categories 2 and 3.

1.4.2 James Reason's Categories

The prominent risk researcher James Reason (Reason, 1997) classifies accidents into two main types. The first type is *individual accidents*, which are accidents that are caused and suffered by single individuals. These types of accidents are relatively common, as can be illustrated by the relatively high number of both road traffic accidents and falls in their homes by elderly people. The second type Reason calls *organizational accidents*. These are fortunately relatively rare, but may have a large-scale impact on populations. Organizational accidents are generally characterized by multiple causes and numerous interactions between different system elements. It is this type of accident that is of main interest in this book. Reason's categories of accidents are also discussed in Section 2.7.2.

Table 1.3 outlines some of the most severe accidents we have witnessed in the last few decades, which all classify as organizational accidents according to Reason's categorization.

1.5 RISK IN OUR MODERN SOCIETY

1.5.1 Increasing Risk

Most safety researchers agree that the risk in our society has been increasing steadily throughout the last two to three decades. Reasons for this trend may include (e.g., see Rasmussen, 1997; Leveson, 2004):

- The very fast pace of technological change and the more and more complex relationships between humans and automation.
- The steadily increasing scale of industrial installations, which increases the potential for large-scale accidents.
- The rapid development of information and communication technology, which leads to a high degree of integration and coupling of systems. This is claimed to improve flexibility, but may also increase the likelihood of accidents.
- The aggressive and competitive environment that companies have to operate in, which encourages higher speed of operation, harder use and less maintenance of equipment, and few buffers.
- The steady demand for higher speed (faster cars, trains, ships, airplanes).
- The increased likelihood of sabotage and terrorism.
- The increasing use of multicultural work forces (often motivated by cost reduction), which may introduce cultural barriers and language problems.

Table 1.3 Some major accidents.

Location of accident	Year	Consequences
Flixborough, UK	1974	Explosion and fire, 27 killed, more than 100 injured.
Seveso, Italy	1976	Dioxin release, 2 000 poisoned, contamination of environment, mass evacuation.
North Sea, Norway	1977	Oil/gas blowout on *Bravo* platform, pollution of sea.
Three Mile Island, USA	1979	Complex accident. Had potential for a major release of radiation.
Newfoundland, Canada	1982	Platform *Ocean Ranger* lost, 84 killed.
Bhopal, India	1984	Release of toxic methyl isocyanate, 3 800 killed, 20 000 injured, 200 000 evacuated.
Mexico City, Mexico	1984	Explosion and fire at LPG storage and distribution depot at San Juan Ixhautepec. Around 500 killed.
USA	1986	Explosion of *Challenger* space shuttle. 7 killed.
Chernobyl, Ukraine	1986	Explosion and atomic fallout at nuclear power station.
Basel, Switzerland	1986	Fire at Sandoz warehouse. Rhine River contaminated, severe environmental damage.
Zeebrügge, Belgium	1987	The car and passenger ferry *Herald of Free Enterprise* capsized. 193 killed.
North Sea, UK	1988	Explosion and fire on the *Piper Alpha* platform. Platform lost, 167 killed.
Pasadena, USA	1989	Explosion and fire, 23 killed, 100 injured.
Alaska, USA	1989	Oil spill from tanker *Exxon Valdez*. Severe environmental damage.
Amsterdam, The Netherlands	1992	Boeing 747 cargo plane crashed near Schipol airport. 43 killed.
Baltic Sea	1994	The car and passenger ferry *Estonia* capsized, claiming 852 lives.
Eschede, Germany	1998	High-speed train derailed. 101 killed, 88 injured.
Longford Australia	1998	Explosion and fire, 2 killed, Melbourne without gas for 19 days.
Bretagne, France	1999	Loss of tanker *Erika*. Major oil spill.
Enschede, The Netherlands	2000	Explosion in fireworks plant. 22 killed, 1 000 injured, more than 300 homes destroyed.
Toulouse, France	2001	Explosion and fire in fertilizer plant. 30 killed, 2 000 injured, 600 homes destroyed.
Galicia, Spain	2002	Loss of tanker *Prestige*, major oil spill.
Texas City, USA	2005	Explosion and fire, 15 killed, 180 injured.
Hertfordshire, UK	2005	Explosion and fire at Buncefield Depot.
Gulf of Mexico	2010	Blowout and explosion on the drilling rig *Deepwater Horizon*. 11 killed, 17 injured, rig lost, major oil spill.

– The emerging climate changes and instability of weather conditions, leading to more frequent and more severe flooding, storms, and so on.

1.5.2 Experience of Major Accidents

During the last three to four decades, a number of major accidents have made the public increasingly aware of the risks posed by certain technical systems and activities. Several accidents have also changed the authorities' attitudes toward such systems. The industry itself is also concerned, since the consequences of such accidents not only incur enormous costs, but may even force a company out of business and seriously damage the image of an entire industry. Examples of accidents with far-reaching effects on the attitudes of regulatory and legislative bodies are listed in Table 1.3.

These accidents are representative of a large number of accidents that have served to remind us that safety can never be taken for granted. Macza (2008) discusses several of these accidents and the society's response to each accident with respect to legislation changes and other actions.

1.6 SAFETY LEGISLATION

Many laws and regulations have emerged or been changed after major accidents, which have called for an increasingly structured approach to safety legislation. Safety legislation has a long history. As early as 1780 B.C., Hammurabi's code of laws in ancient Mesopotamia contained punishments based on a peculiar "harm analogy." Law 229 of this code states:

> If a builder builds a house for someone, and does not construct it properly, and the house that he built falls in and kills its owner, then that builder shall be put to death.

Safety legislation has traditionally been based on a *prescriptive* regulating regime, in which detailed requirements for the design and operation of a plant are specified by the authorities. The trend in many countries is now a move away from such prescriptive requirements toward a *performance-based* regime, which holds the management responsible for ensuring that appropriate safety systems are in place. Hammurabi's law may be the earliest example of a performance-based standard (Macza, 2008). Goal orientation and risk characterization are two major components of modern performance-based regimes, which have been endorsed enthusiastically by international organizations and various industries (Aven and Renn, 2009b).

1.6.1 Safety Case

Several countries have introduced a *safety case* regime. A safety case is a risk management system that requires the operator of a facility to produce a document which:

(a) Identifies the hazards and potential hazardous events.

(b) Describes how the hazardous events are controlled.

(c) Describes the safety management system in place to ensure that the controls are effective and applied consistently.

The detailed content and the application of a safety case vary from country to country, but the following elements are usually important[4]:

- The safety case must identify the safety critical aspects of the facility, both technical and managerial.
- Appropriate performance standards must be defined for the operation of the safety critical aspects.
- The workforce must be involved.
- The safety case is produced in the knowledge that a competent and independent regulator will scrutinize it.

1.6.2 Risk Assessment in Safety Legislation

In Europe, a number of EU directives and regulations have been issued that make it mandatory to carry out various types of risk assessment of a wide range of potentially hazardous systems and activities. This is also the case in other parts of the world. Some main laws are introduced briefly below to illustrate the wide span of application:

- The EU Directive on the control of major accident hazards involving dangerous substances (82/501/EEC) is often referred to as the *Seveso directive* since it was issued in response to the Seveso accident in 1977. The Seveso directive was amended in 1986 and 1988 to take into account the lessons learned from the Bhopal disaster and the Sandoz fire. A more significant revision of the directive was issued in 1996 as a consequence of the Piper Alpha disaster, and is called the *Seveso II directive* (EU, 1996).[5]

  The application of the Seveso II directive depends on the quantities of dangerous substances present (or likely to be present) at an establishment. Two levels ("tiers") of duty are specified in the directive, corresponding to two different quantities (or thresholds) of dangerous substances. Sites exceeding the higher, "upper tier" threshold are subject to more onerous requirements than those that qualify as "lower tier."

  Similar legislation is also implemented in several other countries: for example, as 29 CFR 1910.119, "Process safety management of highly hazardous chemicals," in the United States. This law requires that process hazard analyses (PrHAs) be carried out.

[4]Based on `http//www.nopsa.gov.au`.

[5]In the UK, the Seveso II directive is implemented as the *control of major accident hazard* (COMAH) regulation.

- The EU machinery directive (89/392/EEC) covering safety aspects of a wide range of machines was introduced in 1989. This directive requires that risk analyses are carried out for some dangerous machines, and a specific risk analysis standard, ISO 12100 (2010), has been developed for this purpose. Similar legislation has been implemented in several countries.
- The Health and Safety at Work etc. Act of 1974 (HSWA) is the principal health and safety law in the UK. It places general duties on employers to ensure the health, safety, and welfare of their employees at work, and also to conduct their undertaking in such a manner that persons outside their employment are not exposed to risks. Employers must carry out various risk assessments to ensure that these duties are met "so far as is reasonably practicable" (SFAIRP).
- The Offshore Installations (Safety Case) Regulations 1992, issued by the UK Health and Safety Executive (HSE), require that specific risk assessments be carried out and that a safety case be developed and kept "alive" (i.e., updated).
- The U.S. Maritime Transportation Security Act (2004). This act is designed to protect U.S. ports and waterways from a terrorist attack. It requires vessels and port facilities to conduct risk and vulnerability assessments.
- In Norway, regulations concerning the implementation and use of risk analyses in petroleum activities have been issued by the Petroleum Safety Authority Norway and the Norwegian Ministry of the Environment. A special standard, NORSOK Z-013 (2010), has been developed to support the required risk assessments.

1.6.3 Risk Analysis Standards and Guidelines

A wide range of standards and guidelines for risk analysis have been issued. Some of these are listed in Table 1.4. The list is provided as an illustration and is far from being complete.

1.7 RISK AND DECISION-MAKING

Even though numerous laws and regulations require that risk assessments be carried out, it is important to understand that a risk assessment should never be performed simply to satisfy some regulatory requirement. Rather, it should be performed with the intention of providing information for decision-making about risk.

The objective of almost any risk assessment is to support some form of decision-making where risk is an important decision criterion. Decisions may relate to the following questions (e.g., see HSE, 2001a; Holmgren and Thedén, 2009):

(a) Should the activity be permitted?

(b) Are additional barriers or other system improvements necessary to reduce the risk?

Table 1.4 Standards and guidelines for risk analysis (some examples).

International standards

(a) IEC 60300-3-9: *Dependability Management—Application Guide: Risk Analysis of Technological Systems.*

(b) ISO 12100: *Safety of Machinery—General Principles for Design: Risk Assessment and Risk Reduction.*

(c) ISO 31000: *Risk Management: Principles and Guidelines.*

(d) ISO 31010: *Risk Management: Risk Assessment Techniques.*

(e) ISO 17776: *Petroleum and Natural Gas Industries—Offshore Production Installations: Guidelines on Tools and Techniques for Hazard Identification and Risk Assessment.*

(f) ISO 14971: *Medical Devices: Application of Risk Management to Medical Devices.*

National general standards and guidelines

(a) NS 5814: *Requirements to Risk Assessments*, Norwegian standard.

(b) CAN/CSA-Q634-91: *Risk Analysis Requirements and Guidelines*, Canadian standard.

(c) CAN/CSA-Q850: *Risk Management: Guideline for Decision-Makers*, Canadian standard.

Process industry standards and guidelines

(a) CCPS: *Guidelines for Hazard Evaluation Procedures.*

(b) CCPS: *Guidelines for Chemical Process Quantitative Risk Analysis.*

(c) DOE-HDBK-1100-96: *Chemical Process Hazards Analysis.*

Oil/gas industry standards and guidelines

(a) NORSOK Z-013: *Risk and Emergency Preparedness Analysis.*

Nuclear industry standards and guidelines

(a) NUREG/CR-2300: *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessment for Nuclear Power Plants.*

Space industry standards and guidelines

(a) NASA: *Probabilistic risk assessment procedures guide for NASA managers and practitioners.*

(b) ESA: *Space Product Assurance; Hazard Analysis.*

Railway standards and guidelines

(a) EN 50126: *Railway Applications: The Specification and Demonstration of Reliability, Availability, Maintainability, and Safety (RAMS).*

(b) RSSB: *Engineering Safety Management (The Yellow Book).*

Maritime standards and guidelines

(a) IMO: *Guide for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process.*

(b) ABS: *Guide for Risk Evaluations for the Classification of Marine-Related Facilities.*

Electronics industry guidelines

(a) SEMATECH: *Hazard analysis guide: A reference manual for analyzing safety hazards on semiconductor manufacturing equipment.*

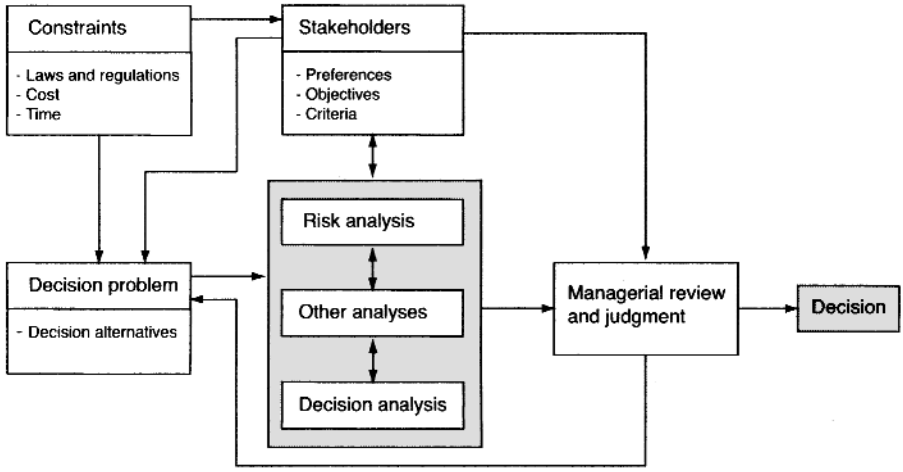

Figure 1.9 Decision framework (adapted from Aven, 2003).

(c) Which of various options, involving different combinations of safety and expenditure, should be preferred?

(d) How much should be invested to improve the safety of the system?

To answer questions like these, the decision-maker must decide if, or when, the system or the activity is *safe enough*. By that we mean that the risk is considered so low that further barriers and other improvements are not required.

1.7.1 Model for Decision-Making

It is important to remember that risk is always only one dimension of a decision problem. Operational, economic, social, political, and environmental considerations may also be important decision criteria. A decision is never made in a vacuum. There are always constraints, such as laws and regulations, time and cost limits, and so on, that need to be adhered to, and there are usually a set of *stakeholders* who have interests in the decision and who will seek to influence the decision-making in different ways. A simple model for decision-making involving risk is illustrated in Figure 1.9, which is an expanded version of a similar figure in Aven (2003, p. 98).

The results from a risk assessment can be used as:

- Direct input to decisions (see Figure 1.9)
- Indirect input to decisions: for example, by influencing stakeholders

The actual decision must be taken by the management and is not part of the risk assessment process as described in this book.

1.7.2 Stakeholders

As illustrated in Figure 1.9, the decision process may be influenced by stakeholders, who may be defined as:

☞ **Stakeholder**: Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity (ISO 31000, 2009).

This definition covers many more than the stakeholders indicated in Figure 1.9: for example, people who are affected by the consequences of a possible accident but who do not have the ability or power to influence the decision.

Categories of Stakeholders. Stakeholders may be classified in many different ways. One such classification is based on the stakeholders' (i) power, (ii) urgency, and (iii) legitimacy. Stakeholders may alternatively be classified as (Yosie and Herbst, 1998):

(a) People who are affected directly by a decision to take action on any issue or project.

(b) People who are interested in a project or activity, want to become involved in the process, and seek an opportunity to provide input.

(c) People who are more generally interested in the process and may seek information.

(d) People who are affected by the outcome of a decision but are unaware of it or do not participate in the stakeholder process.

Some stakeholders may have several roles in relation to the system. The consequences of an accident will be different for various stakeholders, depending on their relation to the assets that are harmed. If a worker is killed in an accident, her husband and children will, for example, get consequences other than those that would be received by her employer.

1.7.3 Deterministic Decision-making

Deterministic decision-making means that decisions are made without any consideration of the likelihood of the possible outcomes. Scenarios are predicted based on a deterministic view of the future, assuming that a bounding set of fault conditions will lead to one undesired end event. To prevent this end event from occurring, the decision-maker relies on traditional engineering principles, such as redundancy, diversity, and safety margins.

1.7.4 Risk-Based Decision-making

Risk-based decision-making (RBDM) is a decision-making process that is based almost solely on the results of a risk assessment. The U.S. Department of Energy defines RBDM as:

☞ **Risk-based decision-making (RBDM)**: A process that uses quantification of risks, costs, and benefits to evaluate and compare decision options competing for limited resources (adapted from US DOE, 1998).

The U.S. Coast Guard gives a detailed description of the RBDM process in the four volumes of USCG (2008). The process can be split into four steps:

1. Establish the decision structure (identify the possible decision options and the factors influencing these).
2. Perform the risk assessment (e.g., as described in this book).
3. Apply the results to risk management decision-making (i.e., assess the possible risk management options and use the information from step 2 in the decision-making).
4. Monitor effectiveness through impact assessment (track the effectiveness of the actions taken to manage the risk and verify that the organization is getting the results expected from the risk management decisions).

USCG (2008) may be consulted for details about the various steps.

1.7.5 Risk-Informed Decision-making

The RBDM approach has been criticized for putting too much focus on probabilistic risk estimates and paying too little attention to deterministic requirements and design principles. To compensate for this weakness, the risk-informed decision-making approach has emerged. This approach may be defined as:

☞ **Risk-informed decision-making (RIDM)**: An approach to decision-making representing a philosophy whereby risk insights are considered together with other factors to establish requirements that better focus the attention on design and operational issues commensurate with their importance to health and safety (adapted from NUREG-1855, 2009).

A slightly different definition is given in NASA (2007). The RIDM process can, according to NUREG-1855 (2009), be carried out in five steps:

1. Define the decision under consideration (including context and boundary conditions).
2. Identify and assess the applicable requirements (laws, regulations, requirements, accepted design principles).
3. Perform risk-informed analysis, consisting of:
   (a) Deterministic analysis (based on engineering principles and experience and prior knowledge).

(b) Probabilistic analysis (i.e., a risk assessment including an uncertainty assessment).

4. Define the implementation and monitoring program. An important part of the decision-making process is to understand the implications of a decision and to guard against any unanticipated adverse effects.

5. Integrated decision. Here the results of steps 1 through 4 are integrated and the decision is made. This requires that the insights obtained from all the other steps of the RIDM process be weighed and combined to reach a conclusion. An essential aspect of the integration is consideration of uncertainties.

The main difference between RBDM and RIDM is that with RBDM, the decisions are based almost solely on the results of the probabilistic risk assessment, whereas following RIDM, the decisions are made on the basis of information from the probabilistic risk assessment as well as from deterministic analyses and technical considerations.

1.7.6 The Validity of Risk Assessment

All risk analyses require a wide range of data and assumptions that may be more or less uncertain. Whenever possible, the data and the assumptions should reflect reality as closely as possible. This is not always feasible, and some decision-makers therefore question the validity of the results from risk analysis. A pertinent answer to this type of question is given by Garrick (2008):

> [...] there is seldom enough data about future events to be absolutely certain about when and where they will occur and what the consequences might be. But "certainty" is seldom necessary to greatly improve the chances of making good decisions.

Whenever possible, assumptions should, however, be made to err on the side of conservatism. Such assumptions, known as "conservative best estimates," are to ensure that the assumptions do not result in underestimation of risk and, ultimately, unsafe decisions (NSW, 2003). Uncertainty in risk assessment is discussed further in Chapter 16.

1.7.7 Closure

It is important to be aware that it is never possible for a system to operate with zero risk. Even if a company may be able to operate without a serious incident ever occurring, the potential will always exist. This is why it is so important for operators to understand the risk they face and to fully appreciate the implications of any changes they make to their operations.

Before we dive further into the realm of risk terminology and assessment methodologies, it should be stressed that a risk assessment is of limited value if it is not going to be used, that is, as a basis for decision-making. A general recommendation is therefore:

If you do not have a specified decision problem, do not carry out any risk assessment!

1.8 STRUCTURE OF THE BOOK

This book has two main parts and one appendix part.

1.8.1 Part I: Introduction to Risk Assessment

The first part has seven chapters, which introduce risk analysis and risk assessment. This introductory chapter has presented the main concepts of the book and placed risk assessment into a decision-making context. The remaining chapters are organized as follows: The main concepts are defined and discussed in Chapter 2 and several examples are given. Various types of hazards and threats related to a system are presented and discussed in Chapter 3. Problems related to quantifying risk are discussed in Chapter 4, and several risk metrics are defined. Several approaches to deciding whether a risk level is acceptable or not are presented. In Chapter 5, risk analysis and risk assessment are set into a risk management framework. The various steps in a risk analysis are presented and discussed briefly, and the competence of the study team and the quality requirements are highlighted. A risk assessment is always influenced by the study team's perception of the potential accidents and accident causation, and accident models are therefore presented and discussed in Chapter 6. Part I is concluded by Chapter 7, which lists and describes the input data that are required for a risk assessment.

1.8.2 Part II: Risk Assessment Methods and Applications

Part II presents the main methods for risk analysis according to a structure that follows the main steps of a risk analysis. Chapter 8 discusses the main features of the various methods, especially how the analysis should be planned, prepared, and reported. Chapter 9 presents a number of methods for hazard identification: among them preliminary hazard analysis (PHA) and HAZOP. Chapter 10 presents methods for cause and frequency analysis, such as fault tree analysis and Bayesian networks, while Chapter 11 presents methods for development of accident scenarios, where event tree analysis is the most common method. Safety barriers are discussed in Chapter 12, and a number of methods for barrier analysis are presented and discussed. Human errors and human reliability are discussed in Chapter 13 together with several models for human reliability assessment. Job safety analysis (JSA) is covered in Chapter 14. This deviates slightly from the main structure of Part II, since JSA is a separate method for analyzing the risk related to a specific job/task. Dependent failures and common-cause failures (CCFs) are discussed in Chapter 15, and several CCF models are presented. The uncertainties related to the results from a risk analysis are often of concern, and this is treated in Chapter 16. Part II is concluded in

Chapter 17 by a historical account and status of the development of risk assessment in some selected application areas.

The various analytical methods are, as far as possible, presented according to a common structure. The description of each method is designed to be self-contained such that you should be able to carry out the analysis without having to read the entire book or search other sources. A consequence of this strategy is that the same information may be found in the description of several methods.

1.8.3 Part III: Appendices

Appendix A presents some main elements of probability theory. An introduction to probability theory is given together with some elements from system reliability and Bayesian methods. If you are not familiar with probability theory, you may find it useful to read this appendix in parallel with the chapters that use probability arguments.

Part III also contains a list of abbreviations and acronyms used in the book and a glossary of the main risk concepts. Many of the terms in the glossary are defined throughout the book. In cases where conflicting definitions are used in the literature, several definitions are listed in the glossary.

Additional material related to the book is available on the web site:

`http://www.ntnu.edu/ross/books/risk`

1.9 ADDITIONAL READING

The following titles are recommended for further study related to Chapter 1.

- *Five steps to risk assessment* (HSE, 2006) gives a very brief but well-structured introduction to risk assessment.
- *Probabilistic risk assessment procedures guide for NASA managers and practitioners* (Stamatelatos et al., 2002a) is developed for space applications but also provides valuable information for other application areas.
- *Risk Analysis in Engineering: Techniques, Tools, and Trends* (Modarres, 2006) is a textbook providing a thorough introduction to risk analysis that can be considered a competitor to the current book. The form and structure of the two books are, however, different.
- *Probabilistic Risk Analysis: Foundations and Methods* (Bedford and Cooke, 2001) is a textbook on risk analysis with a strong focus on probabilistic aspects.
- *Risk Analysis: Assessing Uncertainties Beyond Expected Values and Probabilities* (Aven, 2008) is a monograph that discusses specific conceptual issues related to risk analysis.