

## 1

## Introduction

### 1.1 Risk in Our Modern Society

In the Middle Ages, some of the leading engineers and architects were employed as church builders. In this period, churches changed from being built in the Romanesque style to the Gothic style. This transition implied a move from fairly massive stone structures with thick walls, limited height, and relatively small and few windows to a style with much more slender structures, rising higher, and with more and larger openings in the walls for windows. This technological development had a price, with frequent collapses of the new churches. A prominent example is the collapse of Cathedrale Saint-Pierre de Beauvais in 1284 and then again in 1573 (Murray 1989).

This is a good example of how technology traditionally has evolved, through trying and failing. The church builders of the Middle Ages moved beyond what had been done earlier, and this sometimes led to catastrophic failures.

In the Middle Ages, accidents were seen as acts of God, punishing man for attempting to construct such huge buildings. Today, we have a different view on why accidents occur, and society is not willing to accept failure to the same degree as in the Middle Ages. Accidents result in loss of life or serious environmental damage and are often very expensive. Over the last few decades, concepts and techniques have been developed to help us understand and prevent failures and accidents before they happen, rather than just trying to learn from failures that occur. Application of these techniques is what we normally call *risk analysis* or *risk assessment*.

Risk assessments are systematic studies of what can go wrong in the future, describing it and evaluating if we need to do something to reduce risk. They might have been able to predict and prevent the collapse of the Beauvais Cathedral (Figure 1.1) and the consequences of this if these methods were available in 1284. This book is mainly about methods for performing risk analyses, and the theoretical basis for these.



**Figure 1.1** The Beauvais Cathedral (Source: Photo by David Iliff. License: CC-BY-SA 3.0).

Using a word from everyday language, we may say that risk assessment is a method for systematization of *foresight*. The Merriam-Webster online dictionary defines foresight as “an act of looking forward” and this is exactly what we are trying to do when we analyze risk.

We have now started using terms, such as risk, risk analysis, and risk assessment, without really explaining what they mean. For the purpose of this introductory chapter, it is sufficient with a layman’s understanding, but proper definitions and discussions are given in Chapters 2 and 3.

## 1.2 Important Trends

Many trends in society have led to increased focus on risk and risk assessment. Partly, this is due to increased attention to and reduced willingness to accept risk, partly due to increased risk, and partly due to new and different risk sources being introduced or emerging.

Increased attention and reduced willingness to accept risk often go hand in hand. When accidents occur, in particular serious accidents, the media attention is very high and the interest among the general public is correspondingly high. More rapid and comprehensive access to news about accidents, through the Internet, has further increased our attention (and fear) of accidents.

The increasing focus and our reduced preparedness to accept accidents may be seen as a result of our increasing wealth. In the rich part of the world, many of the dangers that we were exposed to earlier, such as life-threatening diseases, hunger, and war are far less prominent in our lives. Our basic needs are generally well attended to and our attention has therefore turned to other causes of death and losses. This can explain why there are large differences in legislation, regulations, and general attention to risk in rich and poor countries. From this point of view, the expectation that accidents should be avoided can be seen as a result of the increasing standards of living.

Many new trends and developments either increase risk, change existing risk, or introduce new sources of risk. Some examples of different character are given in the following.

- (a) *Higher speed*. In recent decades, high-speed trains have become increasingly common. Higher speed implies more severe consequences if an accident occurs.
- (b) *Increasingly connected computer networks*. More and more devices are linked through the Internet. This does not just apply to computers, but many other devices such as cars, kitchen appliances, power systems, electrical meters, heating systems in homes, and mobile phones. This introduces possibilities for accessing and hacking devices from anywhere in the world. The increased number of connected devices increases the possible consequences and the magnitude of the consequences. With the rapid expansion of the *Internet of things* this problem increases day by day.
- (c) *Increased competition and production pressure* have several aspects that influence risk. Processes are moving faster with less time for preparation and planning, with increasing pressure to be efficient, leaving less time to take care to avoid accidents. Cost cutting may also increase risk.
- (d) *Autonomous systems* is a new technology that changes risk. Less people are involved, meaning that fewer are exposed if an accident should occur. On the other hand, people not directly involved may be more exposed (e.g. pedestrians being hit by autonomous cars). Machines may be more reliable for routine tasks than operators, reducing the probability of making errors, but operators are usually better at adapting to unexpected or unusual circumstances. Autonomous systems are complex, and we may not be able to predict all the ways they can fail.
- (e) *Terrorism* has existed for a long time, but mainly locally. It is only in the last couple of decades that this has become a global phenomenon.
- (f) *Climate change* is a global problem that changes risk in many ways. Risk related to natural hazards changes, with not only more violent storms, frequent flooding but also droughts. The world can be affected in different ways, among others reduced food production and lack of drinking water. This can in turn lead to hunger and more refugees.

To manage the effect of all these changes, we need to understand them and this requires systematic methods to identify them and to analyze them.

### 1.3 Major Accidents

When used in risk research, a *major accident* is an accident with large and even catastrophic consequences. During the previous decades, a number of major accidents have made the public increasingly aware of the risk posed by certain technical systems and activities. A common denominator of these is that they not only have immediate effects in terms of loss of life, environmental damage, or economical effects but also long-term effects by changing the public's and the authorities' attitudes toward the systems that have been involved in the accidents. A result of this is that changes in regulations often are made after major accidents. For companies involved, the consequences of these 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 some past accidents with far-reaching effects are listed in Table 1.1. 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.

Many books give overviews of major accidents (Kletz 2001; Mannan 2012) and investigation reports are often published. In some cases, scientific books are also written about major accidents (e.g. see Hopkins 2000; Vaughan 1996).

### 1.4 History of Risk Assessment

The development of risk assessment is closely related to the development of reliability assessment. The two subjects have many concepts and methods in common, and it is therefore difficult to say what belongs to risk and what belongs to reliability. The origin of the word "risk" and its early usage is thoroughly outlined by Bernstein (1998). A thorough historical account of the more recent history of risk assessment is given by Zackmann (2014). Here, we give only some few highlights. We realize that our presentation is biased because its main focus is delimited to developments in Europe and the United States.

Probabilistic risk assessment as we know it today had its root in the insurance (actuarial) discipline at the end of the nineteenth century. The Swedish actuary Filip Lundberg is considered to be the founder of mathematical risk theory. His first mathematical model for nonlife insurance was presented already in 1909, but was largely ignored till the Swedish professor Harald Cramér in 1930

**Table 1.1** Some past major accidents.

Location of accident	Year	Consequences
North Atlantic	1912	<i>Titanic</i> colliding with an iceberg and sinking, 1500 killed.
Flixborough, UK	1974	Explosion and fire, 28 killed, more than 100 injured.
Seveso, Italy	1976	Dioxin release, 2000 poisoned, contamination of environment, mass evacuation.
North Sea, Norway	1977	Oil/gas blowout on <i>Bravo</i> platform, pollution of sea.
Three Mile Island, USA	1979	Nuclear accident. Limited actual consequences, but had potential for a major release of radiation.
Bhopal, India	1984	Release of toxic gas (MIC), 3800 killed, 500 000 exposed to gas.
Mexico City, Mexico	1984	Explosion and fire at LPG storage and distribution depot at San Juan Ixhauhtepc. Around 500 killed.
USA	1986	Explosion of <i>Challenger</i> 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 <i>Herald of Free Enterprise</i> capsized, 193 killed.
North Sea, UK	1988	Explosion and fire on the <i>Piper Alpha</i> platform. Platform lost, 167 killed.
Alaska, USA	1989	Oil spill from tanker <i>Exxon Valdez</i> . 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 <i>Estonia</i> 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 <i>Erika</i> . Major oil spill.
Enschede, The Netherlands	2000	Explosion in fireworks plant. 22 killed, 1000 injured, more than 300 homes destroyed.
Toulouse, France	2001	Explosion and fire in fertilizer plant, 30 killed, 2000 injured, 600 homes destroyed.

(Continued)

Table 1.1 (Continued)

Location of accident	Year	Consequences
Galicia, Spain	2002	Loss of tanker <i>Prestige</i> , 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 <i>Deepwater Horizon</i> , 11 killed, 17 injured, rig lost, major oil spill.
Fukushima Daiichi, Japan	2011	Release of radioactive material with widespread contamination.
Giglio, Italy	2012	Cruise ship <i>Costa Concordia</i> capsized, 32 killed.
Indonesia/Ethiopia	2018/2019	Two crashes with Boeing 737 MAX, with 189 and 157 fatalities, respectively.

developed his insurance risk theory based on Lundberg's approach. In the following years, Harald Cramér made a series of important contributions to risk and reliability theory.

To become a separate discipline, risk assessment had to wait well into the twentieth century. The book *"Risk, Uncertainty, and Profit"* (Knight 1921) was an impressive landmark. In this book, Knight defined risk as "measurable uncertainty." Another seminal book, *Industrial Accident Prevention: A Scientific Approach* (Heinrich 1931), appeared 10 years later.

During World War II, the German mathematicians Robert Lusser and Eric Pieruschka made important contributions to the quantification of reliability. Their most well-known result was the formula for calculating the reliability of a series system.

The first draft to a standard for risk and reliability emerged in 1949, through the guideline on failure modes and effects analysis (FMEA) that was published by the US military as MIL-P-1629. This guideline was later converted to the military standard MIL-STD-1629A. Another important method, fault tree analysis, was introduced in 1962 by Bell Telephone Laboratories during a reliability study of the launch control system of the intercontinental Minuteman missile.

The military standard MIL-STD-1574A "System safety program for space and missile systems" appeared in 1979 and was transformed to MIL-STD-882 "System safety" in 1987.

Human error was early recognized as an important cause of accidents and the technique for human error rate prediction (THERP) was introduced in 1962, mainly by Alan Swain. THERP was primarily directed toward identification and prevention of human errors in nuclear power plants.

Until 1970, the risk assessments were mainly qualitative. Quantitative aspects entered the scene in parallel to the developments of reliability theory that started from the early 1960s. An impressive early work was the book *“Reliability Theory and Practice”* (Bazovsky 1961). Several new books on reliability theory appeared during the 1960s and set the scene for the introduction of quantitative risk assessments from approximately 1970.

The first attempts to use a HAZOP-like approach to identify deviations and hazards in a chemical plant were made by ICI in 1963, but HAZOP, as we know it today, was not developed until around 1974.

Preliminary hazard analysis was introduced in 1966 as a tool to fulfill the US Department of Defense’s requirement for safety studies in all stages of system development.

Perhaps the most important achievements in the 1970s was the “Reactor Safety Study” (NUREG-75/014 1975). A wide range of new methods and new approaches were developed, either as part of, or inspired by this study. Important methods include the “kinetic tree theory” (KITTT) by William Vesely and models for treatment of common-cause failures (Fleming 1975). The Reactor Safety Study was heavily criticized, but this criticism does not diminish its importance. The risk of nuclear energy was discussed in most Western countries and new education programs in risk and reliability emerged in several countries.

The US Nuclear Regulatory Commission (NRC) has played a very important role in the development of risk assessment. Two major landmarks are the publication of the *“Fault Tree Handbook”* (NUREG-0492) in 1981 and the *“PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessment for Nuclear Power Plants”* (NUREG/CR-2300).

Another US report that led to a lot of risk assessments in many countries was “Critical Foundations: Protecting America’s Infrastructures” that was published by the President’s Commission of Critical Infrastructure Protection in 1997. The infrastructures are exposed to natural hazards, technical failures, as well as deliberate hostile actions. The concepts vulnerability, hazard and threat, and security suddenly became common ingredients in most discussions among risk analysts. In many countries, it became mandatory for all municipalities to carry out “risk and vulnerability analyses” of infrastructure and services.

Many of the developments of risk assessment have been made as a response to major accidents (see Section 1.3). In Europe, two major accidents occurred close to the publishing of the Reactor Safety Study. The first of these, the Flixborough accident occurred in 1974 in North Lincolnshire, UK. It killed 28 people and seriously injured 36 out of a total of 72 people on-site at the time. The casualty figures could have been much higher if the explosion had occurred on a weekday, when the main office area would have been occupied.

The other important accident occurred in 1976 in Seveso approximately 20 km north of Milan in Italy, where an explosion led to the release of a

significant amount of cancer-causing dioxin. Together with the Flixborough accident, the Seveso accident triggered the development of the new EU directive on “the major-accident hazards of certain activities,” which is known as the Seveso directive and was approved in 1982.

In the 1970s and 1980s, a range of laws and regulations on safety and risk emerged in many countries. Two well-known laws are the US Consumer Product Safety Act from 1972 and the UK Health and Safety at Work act from 1974.

Many new organizations were established to prevent accidents. The United Kingdom Atomic Energy Authority (UKAEA) was formed already in 1954. In 1971, UKAEA formed its Safety and Reliability Directorate (SRD). The UKAEA SRD was an active organization and published a range of high-quality reports. One of the central persons in SRD was Frank Reginald Farmer who became famous for the Farmer curve (FN-curve) that was used to illustrate the acceptability of risk. Farmer was also the first editor of the international journal *Reliability Engineering*, the forerunner of the journal *Reliability Engineering and System Safety (RESS)*.

Another early organization was the IEEE Reliability Society that was established already in 1951. This society is responsible for the journal *IEEE Transactions on Reliability*. A forerunner to this journal appeared in 1952 under a different name. It changed name three times and finally got its current name from 1962.

The first scientific society that was dedicated to risk analysis, the Society of Risk Analysis (SRA) was established in 1980 and its associated journal, *Risk Analysis: An International Journal*, appeared in 1981.

### 1.4.1 Norway

In Norway, developments of risk assessment have been made in parallel with the offshore oil and gas activities. The first major oil and gas accident, the Bravo blowout on the Ekofisk field in the North Sea, occurred in 1977. There were no fatalities but a significant release of oil to the sea. First and foremost, this accident was an eye-opener for the authorities and the oil companies who suddenly realized that the oil and gas activities were associated with a very high risk. As a consequence of this accident, the Norwegian Research Council initiated a large research program called Safety Offshore, and the authorities demanded the oil companies to support Norwegian research projects and universities. This requirement was strengthened after the second major accident, the capsizing of the semi-submersible accommodation platform Alexander L. Kielland in 1980, with 123 fatalities.

The support from the Safety Offshore research program and the oil companies produced a number of new academic positions and a comprehensive education program at the Norwegian University of Science and Technology (NTNU) in Trondheim. Both authors of the current book participated in

this development at NTNU. The knowledge gained through this period is an important part of the basis for the book.

## 1.5 Applications of Risk Assessment

The use of risk assessment has increased vastly over the years. A steadily increasing number of legislations, regulations, and standards require or mention risk assessment – and methods are being developed. The increase that we have seen therefore seems to continue into the future.

The prime objective of any risk assessment is to provide decision support. Whenever making a decision that affects risk, a risk assessment helps understanding what the sources of risk are. To illustrate this issue, some typical process industry decisions that can be supported by information from risk assessment are listed.

- (a) *Location of a process plant.* Chemical process plants often handle toxic, flammable, and/or explosive materials (commonly called hazardous materials). Release of these materials may affect people living or working outside the plant. Understanding the risk these people are exposed to is important before making a decision about where to locate a plant.
- (b) *Layout of a process plant.* Release of flammable material may cause fire, and this may spread to other equipment, leading to a far more severe event than the initial fire. Understanding the sources of risk may help us locate the equipment at safe distances from each other.
- (c) *Need for and design of safety systems.* All process plants are protected by a range of safety systems, to reduce pressure in tanks and vessels in emergencies, to isolate equipment that is leaking, to detect fires and gas releases, to extinguish fires, and so on. Risk assessment can help us understand what capabilities and capacities these systems need to have to protect against accidents.
- (d) *Performing maintenance operations.* There is a need for continuous maintenance of equipment in a process plant. Some of the work may represent a risk to the maintenance personnel and to others. Risk assessment can help us plan the work so it can be performed in a safe manner and inform the personnel about the risk involved.
- (e) *Deciding about repairs and modifications.* Equipment that is important for safety may fail during the operation of a plant and we normally want to repair this as quickly as possible. Sometimes, doing the repair may represent a risk, and we need to weigh the risk associated with doing the repair against the risk associated with postponing the repair, for example, until the next major shutdown of the plant. Risk assessment can be used to compare options.

- (f) *Reliable work operations.* Sometimes, work operations may be particularly critical to perform correctly because errors in the performance may have large consequences. Risk assessment can be used to systematically evaluate such work operations, to identify if changes are required.
- (g) *Reductions in manning.* A common situation is that cost cutting leads to reduction in manning in process plants. This can have unwanted effects such as less time to perform work or postponement of work that may be critical to maintain a safe plant. Risk assessment can also be used in situations like these, to determine what the effects are on risk.

These are just some examples of decisions where risk assessment may provide input to the decision-making process. The examples illustrate the wide range of problems that may be addressed, from wider issues such as location of a plant to technical details of how an individual system should be designed, and from purely technical issues to issues involving human and organizational factors.

The range of industries and applications where risk assessment is being used is widening constantly. Some examples are listed in Table 1.2. The table gives some examples and does not pretend to provide a complete picture.

**Table 1.2** Risk arenas that may be subject to risk analysis.

Risk arena	Application or problem area
Hazardous substances	Chemical/process industry, petroleum industry (incl. pipelines), explosives industry, nuclear industry.
Transport	Air traffic (airplanes, helicopters, drones), railways, marine transport, road transport.
Space industry	Space equipment and projects.
Product safety	Technical products, such as machinery, cars, robots, autonomous systems.
Critical infrastructures	Drinking water supply, sewage systems, power grids, communication systems, hospitals and health-care, banking and financial systems.
Medical sector	Medical equipment, robotic surgery, bacteria/viruses.
Work, activity	Industry, agriculture, forestry, sport.
Environmental protection	Pesticides, CO <sub>2</sub> , temperature increases, ocean level increases.
Food safety	Contamination, infection.
Health safety	Cancer, tobacco, alcohol, radiation.
Project risk	Time and cost of large projects (e.g. construction, software development).
Economic/financial	Insurance, investment, financial, enterprise, and project risk.
Security	Sabotage, theft, cyberattacks, espionage, terrorism.

The underlying principles and methods described in this book can be applied to all of the risk arenas in Table 1.2, but there are differences in terminology and methods that may be confusing. This applies, for example, if we compare a risk assessment of hazardous materials with a security risk assessment. Definitions and methods are described in guiding documents, standards, and legislation for different applications. In this book, we try to describe risk assessment in a generic manner and Chapter 20 provides examples from a variety of application areas. In the following section, we specify more precisely what the focus of this book is, and the type of applications we are primarily aiming at.

## 1.6 Objectives, Scope, and Delimitation

This book is written for students, engineers, and analysts engaged in risk assessments, both in the design phase and in the operational phase of systems.

The main objective of the book is to give a thorough introduction to risk assessment and to present the essential theory and the main methods that can be used to perform a risk assessment.

More specific objectives are

- (a) To present and discuss the terminology used in risk assessment. Optimistically, we hope 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 analysis and discuss the applicability, advantages, and limitations of each method.
- (d) To present and discuss some specific problem areas related to risk assessment (e.g. human errors, dependent failures).
- (e) To describe how a risk analysis may be carried out in practice and illustrate some important application areas.

The book is concerned with risk related to (i) A technical or sociotechnical *system*, in which (ii) *events* may occur in the *future*, that have (iii) *unwanted consequences* (iv) to *assets* that we want to protect.

The systems considered may be any type of engineered system, ranging from small machines up to complex process plants or transportation networks.<sup>1</sup> The book does not cover all aspects of risk, but is limited to *accidents* where a sudden event harms one or more *tangible assets*. Adverse effects caused by continuous and long-term exposure to a hazardous environment or hazardous substances (e.g. asbestos) are thus not covered unless the exposure is caused by a specific event (e.g. an explosion).

---

<sup>1</sup> System aspects are discussed in Chapter 4.

When people or the environment is exposed to hazardous chemicals, the risk is traditionally analyzed by *dose–response* models, also called exposure–response relationship. This topic is not covered in the book. The book is concerned with the consequences of accidents, but does not describe how we can calculate or otherwise determine the physical effects of accidents. Examples include the impact energy involved in a collision between two cars, the size and intensity of a fire, or the overpressure generated by an explosion. Instead, the methods focus on the probabilistic aspects of the analysis.

In the financial world, investments involving risk of losing money are often made. 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. In general, events that harm only intangible assets (e.g. finances, reputation, and goodwill) are not covered in the book, unless this (intangible) harm is associated to an event harming a tangible asset.

The main focus of the book is risk assessment *per se*, not how the results from the assessment may be used or misused, but some issues related to risk *management* are discussed briefly in Chapter 7.

The book is mainly focused on the study of *major accident* risk. Many of the methods described may be used to analyze and prevent minor accidents, such as occupational accidents, but this is not the main focus of the book. Risk related to deliberate actions, such as sabotage and cyberattacks, is not a main focus of the book, but an introduction to this increasing problem is given in Chapter 17. Environmental risk and resilience are likewise treated only very briefly.

## 1.7 Problems

- 1.1 Section 1.2 describes some trends that change risk. Take some time to reflect on other technological trends that can increase or reduce risk.
- 1.2 An important basis for all risk analyses is a good understanding of failures and accidents that have occurred earlier. Has there been any recent examples of major accidents? Read about the accidents and identify points that we can learn from to avoid future accidents.
- 1.3 Look for accident investigation reports from one of the accidents that are listed in Table 1.1. In many cases, reports can be found on the Internet. Review the report and see what causes are identified and whether they are related to technical failures, human errors, or organizational aspects.

- 1.4 On the Internet, numerous examples of risk analyses and risk assessments can be found. Search for examples and look at what the content is and what the scope of the analysis is.
- 1.5 Look for examples of legislation, guidelines or standards that require risk assessment in your own country.

## References

- Bazovsky, I. (1961). *Reliability Theory and Practice*. Englewood Cliffs, NJ: Prentice-Hall.
- Bernstein, P.L. (1998). *Against the Gods: The Remarkable Story of Risk*. Hoboken, NJ: Wiley.
- Fleming, K.N. (1975). *A Reliability Model for Common Mode Failures in Redundant Safety Systems*. Tech. Rep. GA-A13284. San Diego, CA: General Atomic Company.
- Heinrich, H.W. (1931). *Industrial Accident Prevention: A Scientific Approach*. New York: McGraw-Hill.
- Hopkins, A. (2000). *Lessons from Longford: The Esso Gas Plant Explosion*. Sydney: CCH Australia.
- Kletz, T. (2001). *Learning from Accidents*, 3e. Abington: Routledge.
- Knight, F.H. (1921). *Risk, Uncertainty and Profit*. New York: Houghton Mifflin.
- Macza, M. (2008). A Canadian perspective of the history of process safety management legislation. 8th International Symposium on Programmable Electronic Systems in Safety-Related Applications, Cologne, Germany.
- Mannan, S. (ed.) (2012). *Lee's Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control*, 4e. Waltham, MA: Butterworth-Heinemann / Elsevier.
- MIL-STD-1629A (1980). Procedures for performing a failure mode, effects, and criticality analysis, *Military standard*. Washington, DC: U.S. Department of Defense.
- Murray, S. (1989). *Beauvais Cathedral: Architecture of Transcendence*. Princeton, NJ: Princeton University Press.
- NUREG-0492 (1981). Fault tree handbook. Washington, DC: U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research.
- NUREG-75/014 (1975). *Reactor safety: an assessment of accident risk in U.S. commercial nuclear power plants*. Technical report NUREG-75/014. Washington, DC: U.S. Nuclear Regulatory Commission.
- Vaughan, D. (1996). *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. Chicago: University of Chicago Press.
- Zackmann, K. (2014). Risk in historical perspective: concepts, contexts, and conjunctions. In: *Risk – A Multidisciplinary Introduction*, Chapter 1 (ed. C. Klüppelberg, D. Straub, and I.M. Welp), 3–35. Heidelberg: Springer-Verlag.

