PART 1

General Concepts and Principles

Chapter 1

Introduction

1.1. What is risk management?

What do we mean when we speak of *risk*? Let us consider the following dictionary definitions:

– *Shorter Oxford English Dictionary*: 1. Hazard, danger; exposure to mischance or peril. 2. The chance or hazard of commercial loss, specially in the case of insured property or goods.

– *Merriam Webster Dictionary*: 1. Possibility of loss or injury: see PERIL. 2. Someone or something that creates or suggests a hazard.

– *Chambers Dictionary*: 1. The chance or possibility of suffering loss, injury, damage, etc; danger. 2. Someone or something likely to cause loss, injury, damage, etc. 3. (insurance) a. the chance of some loss, damage, etc., for which insurance could be claimed; b. the type, usually specified, of such loss, damage, etc., fire risk; c. someone or something thought of as likely (a bad risk) or unlikely (a good risk) to suffer loss, injury, damage, etc.

Using these definitions, we see that the word "risk" may denote a *situation of exposure to hazard*, from which *damage* may result. The notion of risk is thus connected to the notion of *hazard*, a hazard being that which may produce *damage* in the future, in an *uncertain* manner. This definition will be considered in more detail and in a more formal manner in Chapter 2.

This notion of risk is closely linked to human activity, and to human existence in general. Humanity has always been exposed to risks and humans have always generated risks to their environment; efforts to manage these risks came as a natural consequence. These risks have evolved over time, and the attitude taken to risk has evolved in parallel.

In the world of industry, risks need to be mastered for ethical, regulatory and economic reasons. This is the purpose of risk management, which, within a framework specific to each company, consists of:

– identifying risks;

– analyzing risks, that is, studying their consequences and the possibility of their occurrence;

– evaluating and ranking these risks;

– defining a strategy to use with each risk: acceptation or toleration, elimination, reduction, transfer or sharing between multiple actors.

This process is sometimes complex and is often carried out in an iterative manner. The risk management process must also make optimal use of company resources.

The aim of this book is to present the methods habitually used to implement risk management in the context of the production of goods or services. As this type of activity can generate a considerable number of more or less interconnected risks, we will concentrate on certain specified risks.

1.2. Nature of risks

Within the context of a business, we may be faced with a wide variety of risks [DAR 12]. These risks can be grouped into two categories, based on whether they only generate loss or both loss and gain at the same time:

– pure risks only present possibilities of *loss*. They are a result of undesirable events. Their occurrence creates losses for the business, while their non-occurrence does not constitute a gain, and the cost of the damage they can entail will not, *a priori*, increase. Risks associated with the security of goods and human life fall into this category;

– speculative and controlled risks can generate *losses* or *profits*, depending on events and decisions. One example of this type of risk can be found in the management of a company or a project. Decisions need to be taken involving risks. The goal is to increase profit, but a possibility of loss exists. These risks are accepted as they are the result of a choice.

The risks encountered in a business context may also be classified according to the nature of their consequences. For example, we may identify:

– risks with consequences for human health, physical or mental, generally concerning company employees, but also those living in the vicinity of sites of production;

– risks to the social and economic situation of personnel;

– environmental risks that create undesirable effects on the natural environment;

– risks to the mechanisms of production caused by phenomena within or external to the business, including natural phenomena such as flooding or earthquakes;

– risks that may damage commercial relationships, caused, for example, by malfunctions in the production mechanisms, in terms of quality, quantity or time delay;

– judicial risks that may undermine the moral entity constituted by the company, which may be held responsible for damages and thus be the target of judicial proceedings. Based on the nature of the case, we can distinguish between affairs of civil responsibility, in which another entity is subject to damage, intentional or otherwise, and criminal cases, linked to regulatory infractions. The person held responsible in these cases may be the company director, other members of the company or the company itself as a distinct moral entity. In the context of criminal cases, responsibility cannot be transferred using insurance;

– financial risks, with a direct negative impact on company assets.

Note that most of these risks have indirect financial consequences. This is the case, for example, when company goods are destroyed or damaged (in the case of major risks), or in situations where the quality or quantity of production is affected. This also applies to data security, problems of continuity in activities, problems connected with intrusion, etc. Risks of a judicial nature can lead to fines that must be paid, and risks to human health or the environment can result in the payment of damages, although these risks cannot simply be reduced to their financial aspect.

In this book, we will concentrate on risks linked to the mechanisms of production, that is those which create damage as a result of undesirable behaviors in the mechanism. The direct consequences of this type of risk concern human health, the environment and the quality and quantity of production throughput.

NOTE 1.1.– This risk is generally, although not solely, a pure risk. Take, for example, the case of a business using a manufacturing process that presents risks due to the nature of one of the products being used, for example a toxic product that could cause intoxication in humans if not sufficiently contained. A company might wish to adopt an innovative procedure to increase production. The risk linked to the danger inherent in the procedure is a pure risk. The risk linked to the decision to choose the new procedure, however, is a speculative risk, and the risk connected with the use of the site is a controlled risk.

1.3. Evolution of risk management

The methods presented in this book were developed from the 1950s onward in order to respond to a demand for greater mastery of risks, whether at company or society level. To replace these methods in their context, we will now provide a brief overview of the development of approaches to risk management.

The word “risk” has its origins in the Greek substantive “$\rho\iota\zeta\alpha$”, meaning “root”, which gave us the Latin “resecare”, meaning “to cut”. This, in turn, evolved to produce “resecum” in medieval Latin, meaning “reef”, in a maritime context. This led to the following interpretation: the reef is an obstacle that the navigator must, imperatively, avoid.

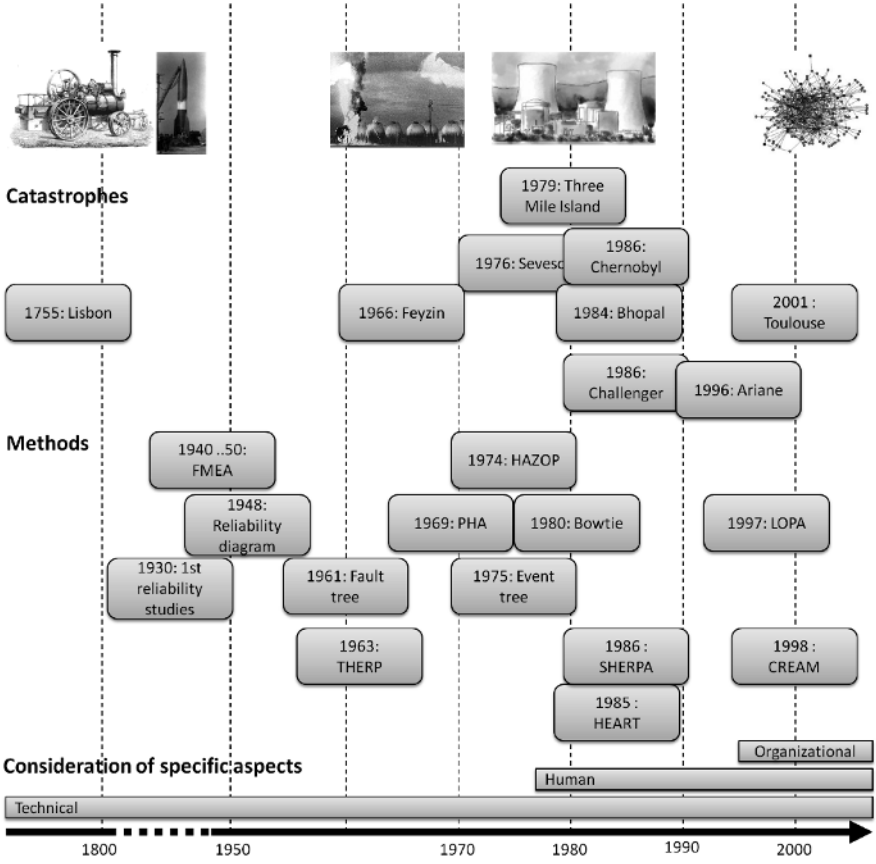

Figure 1.1. *Key points in the history of risk management*

The Lisbon earthquake of 1755, which was followed by a fire and a tsunami, constituted a key event in the development of risk management. A considerable part of the city was destroyed, and between 50,000 and 10,0000 people lost their lives. Faced with this catastrophe, Voltaire placed the blame on nature; Rousseau, however, retorted that "it was not nature which built twenty thousand six- or seven-story houses in that location". Rousseau considered that the problem was due to an error in urban development, implying that risk was not simply the responsibility of the gods, but also that of man.

Later in the 18th Century, Bernoulli, working on the probability theory initiated by Pascal and Fermat in 1654, established the law of large numbers

and formulated his decision theory, introducing the notion of costs weighted by probability.

The 19th Century was marked by the Industrial Revolution, which generated industrial accidents with strong impacts on persons and on the environment. Rail transport also posed security problems, with a first important set of security regulations being established in 1893 (the Railroad Safety Appliance Act).

It was not, however, until the 1930s that the first reliability studies were carried out on the life expectancy of rolling bearings for railroads [VIL 97]. The Weibull distribution appeared in 1939 [WEI 39]. Approaches based on reliability were developed over the course of World War II, during which Lusser and Von Braun's works on the reliability of the V1 and V2 rockets were used to establish a law of reliability for a set of components in series, casting doubts on the weak link law proposed by Pierce in 1926. The notion of failure rate also emerged at this time.

The failure mode and effects analysis (FMEA) method appeared in the late 1940s, first in the military and aeronautical fields.

During the 1950s, with the growing complexity of electronic systems, the Advisory Group on Reliability of Electronic Equipment (AGREE) recommended that reliability should be integrated into the development process in order to promote the design of more reliable equipment. The advisory group also recommended the calculation of indicators such as mean time to failure (MTTF), mean time to repair (MTTR) and mean time between failures (MTBF).

Toward the end of the 1950s, a number of projects demonstrated the importance of human error in system failures. The first analytical forecasts of system reliability including human error and its quantification were published from 1958 onward [WIL 58]: these studies considered human operators as a technical component.

In 1961, H. A. Watson, working at Bell laboratories, developed the fault tree method, allowing the description of the part played by chance or hazard in the operation of complex systems.

The 1970s and 1980s were marked by a number of significant industrial and technological catastrophes:

– Flixborough, 1974: explosion of 50 tons of cyclohexane in a factory producing caprolactame, an intermediary product used in producing nylon, claiming 28 victims.

– Seveso, 1976: a cloud containing dioxine escaped from a reactor in the ICMESA chemical factory, in the town of Meda, and spread across the Lombardy plain in Italy. Four settlements, including Seveso, were affected, with significant consequences on the environment and public health. This event raised public awareness in Europe and resulted in the publication of the SEVESO directive.

– Three Mile Island (TMI), 1979: fusion of a nuclear reactor in the nuclear power plant at TMI, Pennsylvania (United States), with the release of a significant quantity of radioactivity into the environment. The incident was widely reported at international level, and had a major impact on public opinion, particularly in the United States.

– Bhopal, 1984: 40 tons of toxic gas leaked from the Carbide Union pesticide factory in Bhopal (India), killing 8,000 in the first 3 days alone. In total, the leak was responsible for more than 20,000 deaths over a period of almost 20 years. The Bhopal disaster is the most extreme example of a chemical industrial catastrophe to date.

– Challenger, 1986: a solid rocket booster exploded on take-off as a result of a leak caused by a defective O-ring seal. The crew was killed in the explosion. The technical problem was caused by design and organization failures.

– Piper Alpha, 1988: explosion of a North Sea oil rig following a gas leak, causing more than 150 deaths. The accident analysis revealed communication problems during maintenance procedures.

To respond to these major security issues, the industrial world turned to methods developed for electronic systems and in the aeronautic and aerospace domains to study the risks involved in their production facilities. In 1975, the Wash400 report, concerning safety studies in a nuclear power station [NUR 75], introduced the concept of event trees. The report also included fault tree modeling, the use of expert opinions, the inclusion of human error

and feedback analysis. One of the highlighted scenarios corresponded to the TMI catastrophe. The first application of the report to an industrial site was in the context of a study of the Canvey Island complex in 1978 [HSE 78].

From the beginning of the 1980s, operational security techniques were extended to the software domain, where questions of reliability were becoming important as the field underwent rapid expansion. In the context of software design, a number of techniques were developed to enable rapid development of software with maximum reliability. Analysis, design and development procedures focusing on programming languages and methods were defined progressively, in conjunction with formal methods used to guarantee correct operation of software.

During the same period, new methods were developed to analyze the reliability and availability of systems, taking account of dynamic aspects using Markov chains and Petri networks.

The 1980s also witnessed the development of several new methods for including the human factor, such as the technique for the human error rate prediction (THERP) method (see Chapter 14).

In the course of the 1990s, risk analysis developed in a number of domains, including the automotive industry, civil engineering and building. Work was also carried out on the impact of organization, with the addition of an organizational aspect to considerations of human factors. The theories of normal accidents [PER 99] and high reliability organizations [ROB 90] were also developed at this time.

In France, the beginning of the 21st Century was marked by the AZF catastrophe, where a stock of ammonium nitrate exploded at a factory in Toulouse. This led to the creation of the law of 30th July 2003 on the prevention of technological risks. In parallel, the development of safety instrumented system and their generalization within the framework of the IEC 61508 standard led to the use of new methods, such as the bow-tie diagram at the center of the Accidental Risk Assessment Methodology for Industries in the framework of the Seveso II Directive (ARAMIS) method or the layer of protection analysis (LOPA) method, which allows a probabilistic study of accident scenarios and an evaluation of the effectiveness of security barriers.

In parallel to the development of these methods, a strategy for reflection was established using a subjective, rather than objective, vision of risk. Using an objective vision, the level of risk was considered to be independent of the observer, that is as a value that may be measured in a unique and universal manner by any observer with the requisite knowledge. This approach was re-examined by certain authors [REN 92, SLO 01, DEN 98], who proposed a subjective vision in which risk ceases to be an objective element, but rather a perceived element: the level of perceived risk depends on the observer, on what they consider to be reliable or otherwise, their intuition, their culture, media influence, etc. This is true of the general public, but is also applicable to experts. Moreover, despite the apparent objectivity of mathematical and probabilistic approaches, results are rarely used in their raw form in decision making, as a significant degree of uncertainty exists concerning available data [REI 99]. It is a mixture of the two approaches that can be found in Ren [REN 98].

In the context of this book, we will retain this latter point of view. The methods we will present are those generally used for risk analysis in structures producing goods and/or services. They allow us to obtain a measurement of risk, with a representation of the level of risk as a position on a probability–severity diagram (Figure 1.2). The results obtained in this way are not absolute, and should be interpreted with care. However, these results constitute an element for risk analysis which may serve as a point of reference, notably from a regulatory standpoint.

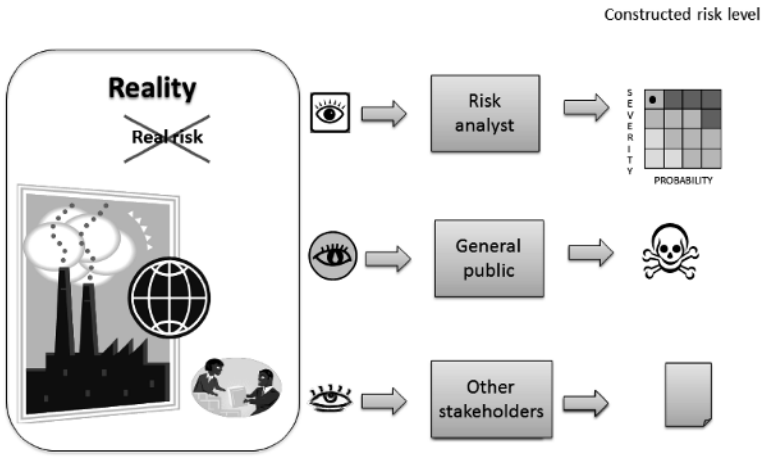

Figure 1.2. *Representation of risk*

1.4. Aims of this book

The objective of this book is to present the methods used for risk analysis in production systems. We will begin by presenting a certain number of basic notions, and then the general principle of risk analysis. Following on from this, we will examine the ISO31000 standard, which provides a specification for the implementation of a risk management approach.

The ability to represent the information we use is crucial, so we will also consider the representation of knowledge, covering both information concerning the risk occurrence mechanism and details of the system under scrutiny.

We will then present different analysis methods, first for the identification of risks, then for their analysis in terms of cause and effect and finally for the implementation of security measures.