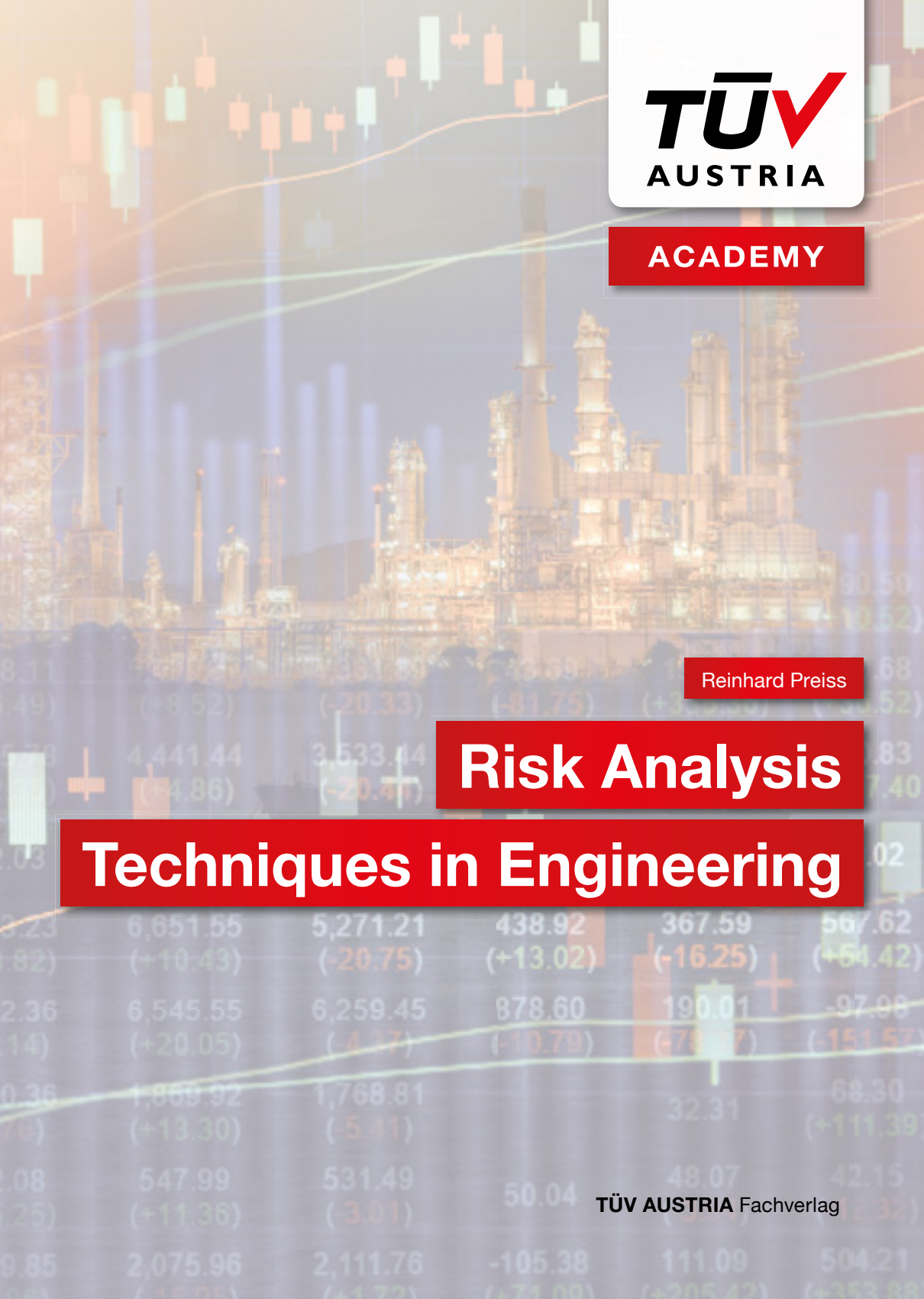

TÜV AUSTRIA

ACADEMY

Reinhard Preiss

Risk Analysis Techniques in Engineering

TÜV AUSTRIA Fachverlag

Risk Analysis Techniques in Engineering

ISBN 978-3-901942-82-2

Author: Dr. Reinhard Preiss, Executive Business Director Industry & Energy,
TÜV AUSTRIA GROUP

Published by
TÜV AUSTRIA AKADEMIE GMBH
Leitung: Mag. (FH) Christian Bayer, DI (FH) Andreas Dvorak , MSc
2345 Brunn am Gebirge, TÜV AUSTRIA-Platz 1
+43 5 0454-8000
academy@tuv.at | www.tuv-academy.at

Project Management: Mag. Judith Martiska
Layout: Mag. Evelyn Hörl
Production: druckwelten.at
Cover: Markus Rothbauer; Foto: Adobe Stock

© 2020 TÜV AUSTRIA AKADEMIE GMBH

The work is protected by copyright. All rights, in particular the rights of distribution, duplication, translation, reprinting and reproduction, remain reserved to the publisher, even if they are used only in extracts.
No part of the work may be reproduced in any form (by photocopy, microfilm or any other process) or stored, processed, reproduced or distributed using electronic systems without the written permission of the media owner.
Despite careful examination of all contributions in this work, errors can not be ruled out. The correctness of the content is therefore unaware. A liability of the publisher or authors is excluded.

Making complexity understandable

Today companies are faced with a number of challenges: Besides existing market requirements, social demands on businesses have grown that go far beyond the maintenance and creation of jobs in recent years.

Added to this – as an expression of the socio-political claim on companies – are legal framework conditions that are becoming increasingly complex and will tie up resources. Correspondingly, many companies – and the industry as a whole – often and quite rightly complain about a hardly manageable flood of regulations.

Companies are often challenged to find dynamic, adaptable solutions in this environment for themselves, especially concerning security.

Assessing risks of technical systems to avert harm to people and environment naturally plays a significant role and is particularly important for the industry.

After all, "security" is no longer a determining factor only for employees but features as an important quality asset in international competition for the business and industrial location.

In addition, there are the challenges in data security, which are gaining importance due to the dynamic development of digitization in production.

Against this background, not only the vehement demands for de-bureaucracy and deregulation are understandable. Besides economic policy conditions, the topics of risk analysis and risk management are growing in significance. Understanding methods of risk analysis and risk management and preparing them as a tool for companies is just the kind of valuable support that businesses need in an increasingly complex environment.

Mag. Christoph Neumayer

General Secretary
Industriellenvereinigung

Preface

Nothing is as constant as change. This quote attributed to Heraclitus of Ephesus is more valid today than ever. In times of change, paradoxically, people's need for safety and security increases. Some authors like to talk about the so-called "comprehensive insurance cover society" in this context. However, absolute security is something unattainable, especially in complex technical systems.

Anton Neuhausler has aptly stated: "There is no certainty, only different degrees of uncertainty." In order to cut through this Gordian knot consisting of safety needs and practical possibilities, the methods for systematic risk identification and assessment have been developed considerably in the recent past.

The book Risk Analyses Techniques in Engineering on hand in its updated and extended 2nd edition provides an overview of the current state of the art in risk analysis and will prove to be a valuable and practical guide on safety issues, giving an insight on how to meet the increased security requirements with a technically feasible effort.

I hope that the book is distributed widely and above all that it contributes to the systematic improvement of safety.

Dir. Dipl.-Ing. Dr. Stefan Haas

CEO
TÜV AUSTRIA HOLDING AG

Foreword of the Author

The systematic analysis and evaluation of the risks associated with technical systems has long been a standard procedure in the high-risk sectors like the chemical industry, oil and gas industry, aviation, and medical engineering. Due to the existing and constantly increasing legislative, normative and liability requirements, application of systematic methods of risk analysis and evaluation, ultimately the entire risk management process, is now required in almost all the areas of engineering.

Its objectives include prevention of harm to people, environment and property and ensuring the required availability of technical systems and processes, thereby taking care of the ethical responsibility of engineering, besides ensuring competitiveness of the technical systems. The estimated costs of disasters exceed the costs for implementing risk minimizing systems enormously. Therefore, saving in cost of risk minimisation can be termed in many cases as short-sighted and uneconomical and is unacceptable both socially and legally in the event of damage to people or environment.

This book should make its contribution in explaining the common methods of risk analysis and management to promote their wide use.

The second edition throws light on a wide range of methods now explained in greater details, with more examples of their application besides highlighting the basics principles underlying the use of newer methods like for example Human Error Analysis and Risk Based Inspection (RBI), the mistakes in the first edition have also been corrected.

At this point, I would especially like to thank my colleague Dr. Joachim Rajek, who has contributed the chapter dealing with Risk Based Inspection. His expertise in this area has given an added value to this book, particularly with respect to its application in the area of process industries.

Dipl.-Ing. Dr. Reinhard Preiss

Executive Business Director Industry & Energy
TÜV AUSTRIA GROUP

Table of Contents

1 Introduction

1.1 General

This chapter is an introduction to the field of risk analysis in engineering. It includes basic definitions of the terms and describes the correlation between the analyses and the concept of risk management, besides highlighting the typical areas of its application and their legal context.

Risk management covers all the measures for a systematic identification, analysis, evaluation, monitoring and managing the risks of an organisation and describes its management process. The technical risk analysis is used in this context for identification and evaluation of risks that influence or can affect the safety of technical systems and thereby interfere with the goals of the organisation (e.g. with respect to industrial, individual and environmental safety etc.).

The term risk analysis (in engineering), used in the title of the book, is a collective term for the identification, analysis, evaluation and managing (taking measures) technical risks.

The following areas can be considered typical for application of technical risk analysis:

- ✓ product safety and product liability
- ✓ employee and environmental safety
- ✓ process safety
- ✓ safety of critical infrastructure

There are certainly more areas – for instance particularly the aerospace, rail and other mass transport industries as well as medical engineering – in which the technical risk analysis can make an important contribution in designing and ensuring the safety of the systems.

The primary goals of risk analysis in engineering are:

- ✓ prevention of personal injury
- ✓ prevention of environmental damage and damage to property
- ✓ prevention of damage to image and reputation caused by errors or failures of products and equipments
- ✓ increasing the availability reliability and efficiency of systems, equipments and processes

Especially the **legal security** achieved through the analysis and documentation of the risks and the measures to reduce them is of prime importance to all the concerned parties.

With reference to the foreword, the terms **known/unknown**, **knowns/unknowns** have been elaborated and explained with the help of examples at the end of the chapter (as theoretical motivation).

1.2 Terminology

Some important terms that keep appearing repeatedly with reference to risk analysis in engineering have been either explained or defined below. A common understanding and a common language of people dealing with the concept of risk and risk analysis in engineering, is an important prerequisite for achieving right and consistent results.

Danger

Condition or characteristic with the potential to cause a negative impact on humans, environment or material; is a broad non-specific term.

Hazard

A danger, as indicated for a specific situation; specific in terms of time and location for the concerned person or asset or environment; poses a potential source of harm.

> Note: The aforementioned definitions of the terms danger and hazard, very often used in process engineering, differ in meaning from that in [Ref. 1-1].

Risk

A classical universal definition, as given in [Ref. 1-1], [Ref. 1-2], [Ref. 1-3]: "Effect of uncertainty on the goals".

However, in engineering, the term "risk" is normally interpreted as the probability of occurrence of a loss and the severity of this loss; the magnitude can be determined only for a specific situation with specific parameters.

> Colloquial: risk = function (consequences, probability of occurrence of these consequences).

A universally accepted definition is also as per: [Ref. 1-26]: "Risk is a measure of human injury, environmental damage, or economic loss in terms of both the probability of occurrence and the magnitude of the loss or injury".

Probability

The degree at which an event (damaging event) probably occurs. The probability can be understood with reference to a period (e.g. probability for a year, or with reference to the lifespan) or to the number of events (event probability, often expressed in percentage). When used with reference to a period, often the term "frequency" is used e.g. "once in 100 years".

Risk analysis

Systematic evaluation of the available information to identify the hazards, and the risks associated with them and then assess them according to their magnitude (i.e. with reference to the probability of occurrence and the consequence).

Risk evaluation

Comparing risks with predefined threshold values.

Risk assessment

Collective term for risk analysis and risk evaluation.

Risk area; Boundary of risk area

Areas/limits in the risk landscape (small, medium, big risks); the risk tolerance limit and/or he risk acceptance limit separate the risk areas from each other.

Residual risk

Risk that remains even after implementing the safety measures (risk reduction measures).

Acceptable risk

Risk that is acceptable in a certain context with respect to the basic and/or moral concepts of an organisation. Additional measures to reduce the risk are not considered as necessary.

Tolerable risk

Risk, which is tolerated by the concerned persons or organisations taking into consideration the advantages of the risky systems or technology.

However, this term differs from the generally acceptable risk as the tolerance can be varying depending upon the concerned group of people. Additional measures to reduce the risks are normally considered in the context of their cost-benefit equation.

Unacceptable risk

Risk that lies beyond (above) the tolerance limit. Additional measures to reduce the risk are obligatory.

ALARP

Reduction of risk "as low as reasonably practicable". Implementing measures to reduce a risk so that the residual risk is not unacceptable and the cost of every additional measure for minimising the risk is excessively high compared to the further reduction of the risk [Ref. 1-4].

However, the cost-benefit relation cannot be used to implemenmt risk reduction measures which are below the corresponding good industrial standard (at least for risks which might lead to harm to people or the environment)

Mitigation

Measures to reduce the impact of a hazardous event.

Prevention

Measures to reduce the frequency of the occurrence of a hazardous event

Example

Danger: Sulphuric acid

Hazard: Tank with 1,000 l sulphuric acid in a storage tank

Consequence: Spilling of sulphuric acid due to overfilling resulting in an injury of a person and environmental pollution due to its spreading in ground water

Risk: Function of the probability of overfilling and of the consequences of spilling

Mitigation: Tank dyke

Prevention: Controlling of the filling level, liquid level-high-alarm with automatic inflow cut off

Qualitative risk analysis

Risk analysis and description of a risk, or the evaluation of the residual risk, which is not based on clearly defined quantitative variables, especially with reference to the probability of occurrence. Using qualitative keywords like for example unknown-seldom-frequent-continuous (probability of occurrence, frequency), negligible-low-moderate-catastrophic (consequence), etc. For further details and examples of application refer to chapter Risk evaluation.

Quantitative risk analysis

Risk analysis and description of a risk, or the assessment of the residual risk, on the basis of clearly defined quantitative variables, for example the extent of damage in Euros or the number of people affected/degree of injury, and probability of occurrence denoted as frequency (instances per time unit). For further details and examples of application refer to chapter Risk Evaluation.

Note: In process safety, the abbreviation QRA (Quantitative Risk Assessment) stands for a standardised process, based on mathematical methods, for indicating the probability of occurrence and the consequences of serious accidents affecting the operation of a plant and its environment. Also refer to chapter 17.

Semi-quantitative risk analysis

Risk analysis and description of a risk, or the evaluation of the residual risk, on the basis of calibrated figures, for example using RPN (Risk Priority Number) for FMECA, or 3-F method or Dow Fire & Explosion Index.

Occasionally, quantitative analysis (according to the above definition) is also called as semi-quantitative analysis, when the probability of occurrence or the consequences are not indicated explicitly and are given only in terms of a numerical range (or as magnitude). For further details refer to the description of the specified methods.

Event

Ein Ereignis im Rahmen eines Vorganges (Prozesses), welches zu einer Abweichung vom normalen Zustand und in weiterer Folge möglicherweise zum Verlust der Kontrolle über eine Gefährdung führt.

An event, as a part of a process leading to a deviation from the normal condition and which may possibly further lead to loss of control over a hazard.

Consequence

Extent of damage caused by an event.

Scenario

An event or multiple events leading to or which can lead to an undesired consequence.

Risk management process

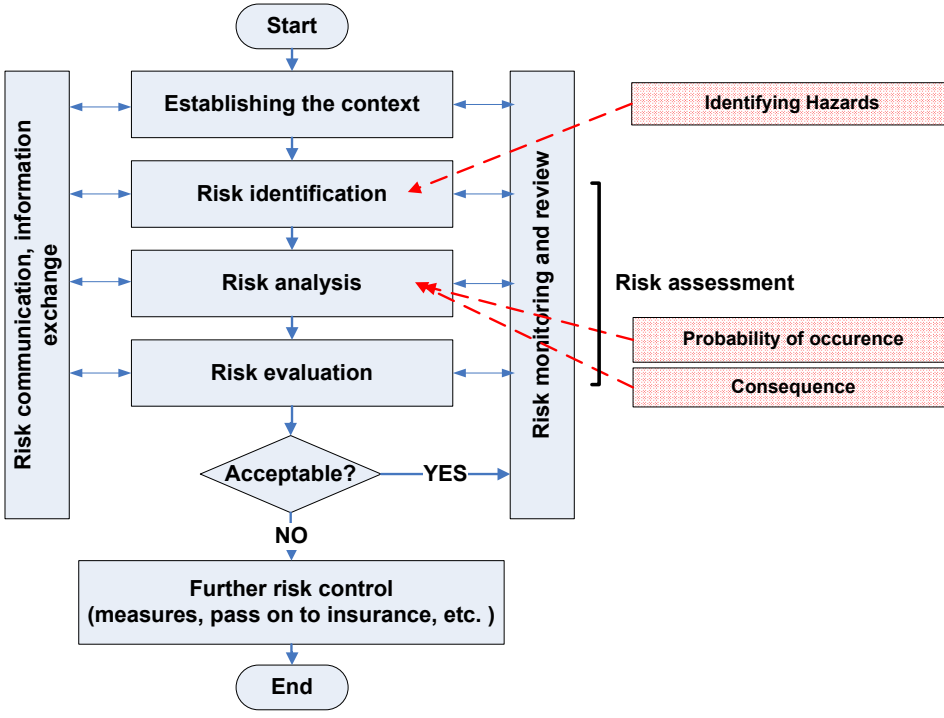

Figure 1-1: Risk analysis and evaluation as a part of risk management process

Crisis management

Coordinated activities which an organisation has to carry out to deal with imminent or already occurring crises. In this context, a crisis is a situation, which requires special measures across the organisation, as the existing structures and processes cannot deal with it adequately.

Risk management

Processes and practices aimed at managing an organisation with reference to risks.

Risk owner

Person with executive powers to manage risk. The risk owner can change the risk.

RAM analysis

Reliability, availability und maintainability analysis. Is carried out for equipments in the planning stage to determine the configuration (e.g. redundancies), the required maintenance, spare parts stock, etc. in order to achieve or prove the availability of the equipments (e.g. 99.9 %) as per a given specification. The analysis is based on statistically existing or assumed failure rates of individual components of the equipments.

Corporate Security

Tasks of organisations and systems that are related to security against intentional hazards (caused deliberately by people) [Ref. 1-20].

1.3 Risk analyses as a part of risk management

1.3.1 Overview

According to ISO 31000 [Ref. 1-2], organisations are subject to various internal and external factors and influences, which make it uncertain, when and whether they can achieve their goals. The effect of this uncertainty on the goals of an organisation is termed as “risk”.

Risks form a part of all the activities of an organisation. Organisations manage these risks by identifying, analysing and then evaluating, whether there is a need to change the risk through measures of risk management in such a way that it complies with the respective risk criteria. During the entire risk-management process they communicate with the stake holders, consult them, monitor and review the risks and their change management in order to ensure that no further measures are required for managing the risk. A detailed description of this systematic and logical process is provided by ISO 31000 [Ref. 1-2] and ONR 49000 [Ref. 1-1].

In Figure 1-2, ONR 49000 [Ref. 1-1] describes the focus of an organisation on its goals and strategies and the commitment of its top management and executives in applying the risk management process for management functions, as an essential requirement of effective risk management. Risk management process covers the tasks aimed at managing and monitoring an organisation with respect to the risks. Defining the parameters, identifying, analysing and evaluating risks and managing them along with risk communication and risk monitoring form the crux of this process.

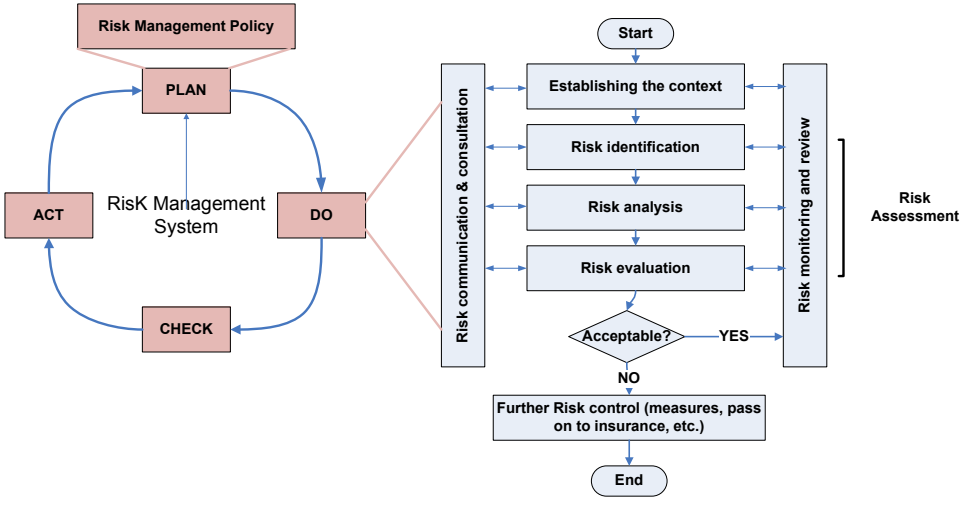

Figure 1-2: Risk management system and process

For introducing the risk management process, to run it effectively, to maintain it and for a consistent improvement, big and complex organisations require an organisational framework which is called as risk management system.

The risk management system includes all the elements of the management system of an organisation, which have the task of managing risks. It describes the managerial functions in an organisation and involves planning, implementing, evaluating and consistent improvement, which can also be described as "plan – do – check – act" (as usual in case of other management systems).

The possible individual aspects of elements of the risk management process are cited below with examples:

Establishing the context

It is important to define the goals, strategies, scope and the factors influencing the operations of an organisation or of everything that forms a part of it, where the risk management process is applied. The resources required for risk management, the responsibilities and authorizations and the related documentation should be specified.

The following aspects have to be taken into consideration:

- ✓ defining the responsibilities for the risk management process
- ✓ defining the scope and application of the risk management activities (e.g. with respect to activities, processes and products etc.)
- ✓ clarification of the relationship between the risk management process and other projects or activities of the organisation
- ✓ defining the methods of risk assessment, especially with reference to life cycle, methodology, details of execution, documentation and updates. It involves determining the analysis required for it, its scope, its scale, goals and the required resources.
- ✓ defining the risk criteria: Definitions can be derived from legal, regulatory or other requirements (e.g. organization internal obligatory ones). Decisions regarding the consistent review of the risk criteria and the usage (e.g. with respect to the best available technology) should be taken. Risk acceptance and tolerance limits should be defined clearly.
- ✓ defining the methodology of risk evaluation (e.g. matrix, graph, ranking, etc.) or modifying it according to the use case, if necessary
- ✓ defining the method for evaluating the performance and efficiency of risk management
- ✓ describing the strategy regarding combination of risks

Risk identification

The aim of the corresponding structured process is to ensure a comprehensive and systematic identification of risks (or hazards underlying the risks), specific for the respective issue. In this case, a prior definition of basic conditions is useful, for example:

- ✓ common sources of risks within and outside the organisation
- ✓ methodology for identifying, if necessary diversified per use case and/or phases of the life cycle
- ✓ availability of information for identifying the risks
- ✓ required technical and other competence of the personnel involved in the process

Risk analysis

The risk analysis should provide a deeper insight into the risk. Risk analysis is an input for risk evaluation and in deciding what strategies and methods are most appropriate for its management.

In addition, risk analysis can also contribute in deciding between multiple options, which include risks of different types having different risk levels.

Risk analysis studies the causes and sources of risks, their effect and the probability of their occurrence. Factors influencing the effect and probabilities should be identified.

As per the applied methodology or initially a common method of determining the effects and the probability of occurrence of scenarios should be defined.

If necessary, a (prior-)standardisation of the risk reduction of safety measures should be carried out.

Risk evaluation

During risk evaluation, the risk level, determined in the risk analysis, is compared with the risk criteria (e.g. evaluation methods, acceptance or tolerance limits), which are defined in the context. Based on this, the need for risk control can be identified.

Risk control and handling

Risk control and handling involves selecting and implementing one or more options to cope with the risks. For example,

- ✓ avoidance of the risk source
- ✓ acceptance or tolerance under permanent/periodic controlling
- ✓ reduction of consequences or/and probability of occurrence through technical/organisational measures.
- ✓ transferring the risk (e.g. by means of an insurance)
- ✓ documentation and communication concerning residual risks

Risk monitoring

An important goal is to ensure the integrity of risk control measures. In addition, events, developments, and changes have to be monitored and analysed continuously to identify any changes in the nature or magnitude of the risk. This includes:

- ✓ product monitoring
- ✓ process monitoring
- ✓ analysis of occurrences
- ✓ management of change
- ✓ periodic re-evaluation of risks

1.3.2 HSE/OI management in the process industry

Many organisations in the process industries, especially in the energy sector (oil and gas) regulate the responsibilities and processes with respect to health, safety and environment or with respect to operational integrity (a process by which health, saftey, environmental sustainability and productivity are ensured) in special management systems.

An HSE/OI management system (H – Health, S – Safety, E – Environmental; O – Operational, I – Integrity) is a structured collection of guidelines, methods and processes, which a company uses to implement the risk management efficiently and successfully.

A system of this kind is represented below as an example (it might differ from actual systems of larger industrial companies in some details, but the basics are the same), and the individual elements are briefly summarized.

11 elements of HSE/OI management system

Figure 1-3: HSE/OI management system