

Protective systems against hazards

Nature and extent of the problem



Protective systems against hazards

Nature and extent of the problem

Technical report prepared by a Working Group
of former FIP Commission 8

October 1999

Subject to priorities defined by the Steering Committee and the Praesidium, the results of <i>fib</i> 's work in Commissions and Task Groups are published in a continuously numbered series of technical publications called 'Bulletins'. The following categories are used:	
category	minimum approval procedure required prior to publication
Technical Report	approved by a Task Group and the Chairpersons of the Commission
State-of-Art report	approved by a Commission
Manual or Guide (to good practice)	approved by the Steering Committee of <i>fib</i> or its Publication Board
Recommendation	approved by the Council of <i>fib</i>
Model Code	approved by the General Assembly of <i>fib</i>
Any publication not having met the above requirements will be clearly identified as preliminary draft.	
This Bulletin N° 5 has been approved as a <i>fib</i> technical report in April 1999 by <i>fib</i> Commission 3 'Environmental aspects of design and construction'.	

The former FIP Working Group on 'Protective systems against hazards' started in 1988. CEB and FIP merged in 1998 into *fib*. This report, therefore, was published in the new *fib* series of bulletins:

K. van Breugel* (The Netherlands, chairman of Working Group), H. Bomhard* (Germany, chairman of former FIP Commission 8 'Concrete Storage Vessel Systems', later named 'Concrete and Environment'), S. R. Close* (USA), M. Fenz † (Austria), A. R. Frankson (USA), H. R. Ganz (France), I. Jorgensen (USA), V. Kaltofen* (Germany), P. Marti (Switzerland), J. Nemet (Austria), G. Opschoor (The Netherlands), V. Papenhausen (Germany), M. Ronde (The Netherlands), D. Rudat* (Germany)

* Main contributors to this publication

Full affiliation details of most Task Groups members may be found in the *fib* Directory.

Cover photo: Risk spectra (according to Bomhard, see fig. 2.4 and Reference 11)

© fédération internationale du béton (*fib*), 1999

Although the International Federation for Structural Concrete *fib* - fédération internationale du béton - created from CEB and FIP, does its best to ensure that any information given is accurate, no liability or responsibility of any kind (including liability for negligence) is accepted in this respect by the organisation, its members, servants or agents.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission.

First published 1999 by the International Federation for Structural Concrete (*fib*)

Post address: Case Postale 88, CH-1015 Lausanne, Switzerland

Street address: Federal Institute of Technology Lausanne - EPFL, Département Génie Civil

Tel (+41.21) 693 2747, Fax (+41.21) 693 5884, E-mail fib@epfl.ch

ISSN 1562-3610

ISBN 2-88394-045-2

Printed by Sprint-Druck Stuttgart

List of Contents		page
Foreword and Executive Summary		iv
Preface		vi
Chapter 1 Introduction		
1.1	The environment in danger	1
1.2	Picturing the problem	1
1.3	Solutions	4
1.4	Protective structures	5
Chapter 2 Safety Concepts - The role of structural protective systems		
2.1	Safety concepts	7
2.2	The risk concept	7
2.3	Consequence control	11
2.4	Safety promoting methods	12
2.5	System Technology	14
2.6	Structural protective systems	14
2.7	Why concrete protective structures?	16
2.8	Deterministic levels of protection	17
2.9	Merits of protective systems	18
2.10	Summary	19
Chapter 3 Hazard Actions		
3.1	General	21
3.2	Blast	21
3.3	Thermal actions	23
3.4	Impacts	25
3.5	Earthquakes	28
3.6	Natural phenomena	29
3.7	Hazardous materials	29
Chapter 4 Hazards Scenarios		
4.1	Scenario thinking	35
4.2	Industrial accidents	35
4.3	Hazard scenario schemes	37
4.4	Examples of waste hazard scenarios	38
Chapter 5 Examples and Developments		
5.1	Introduction	43
5.2	LPG-storage tank	43
5.3	Inground and in-pit solutions	44
5.4	A-seismic design of tank systems	44
5.5	Prestressed concrete pressure vessels	45
5.6	Blast resistant control building	46
5.7	Multi-barrier waste storage system	48
5.8	Buried multi-barrier storage systems	52
5.9	Final comments	53
References		55

Foreword and Executive Summary

In every society, risks are being permanently produced. New kinds of technical developments and new means of satisfying needs create permanent risks. This is particularly noticeable when societies develop into service societies. These embody an enormous increase in prosperity, but at the same time make necessary a super-industrialisation with a greatly increased danger potential. For some time now the risk potential in our highly technically industrialised world has been growing more quickly than investments in safety measures. This makes society more vulnerable and implies danger. A measure of the size of danger is given with the term “risk”, and protection is a form of preventive measures to avert danger.

The risk R is usually defined as the product of the probability P_f of a damaging event and the consequential damage C of the event: $R = P_f \times C$. Below a limit delineated by the relevant practical experience, all indications of probability have a purely hypothetical, speculative character. All damaging events beyond a still tolerable consequential damage C_{limit} represent catastrophic events that must be avoided (see Figure 2.4).

Therewith we are concerned with great differences in risk categories. I will elaborate this by discussing characteristic risk structures:

- Risk category 1.
Usual structures risks with normal damage potential, e.g.:
 - bridges;
 - high-rise buildings, etc.
- Category 2.
Large-scale industrial risks with catastrophic risk potential, e.g.:
 - Mexico City 1984, the catastrophe involving liquid gas;
 - Bhopal/India 1985, the catastrophe involving methylisocyanate;
 - Seveso;
 - Sandoz, etc.
- Risk category 3.
Large-scale industrial risks with catastrophic risk potential, but with a probability of occurrence that cannot be quantified, e.g.:
 - storage and reactor systems for material of unknown composition and effect, for example wastes, irrespective of whether they are of industrial or household origin.
- Risk category 4.
Large-scale industrial risks with a very high damage potential, $C \rightarrow \infty$, and a very small probability of occurrence, $P_f \rightarrow 0$, e.g.:
 - nuclear power plants.

Risks of categories 3 and 4 make clear the weakness of our present safety philosophy, which means safety on the basis of the risk involved. In both categories the risk R cannot be quantified – not for category 3, because the probability of failure, for example of a container for materials with an unknown composition and effect – for example a landfill for wastes – is not quantifiable, and not for category 4, because the situation “zero multiplied by infinity” is singular and can mean anything. Risks of category 2 can, this is true, be quantified, but catastrophes such as those in Mexico City and in Bhopal are not acceptable either.

To take precaution against risks causing catastrophic damage is indispensable also under ecological, economical and social aspects according to the paradigm of sustainability dictated by the Agenda 21 signed in Rio 1992 by 179 nations.

Under these circumstances, protection cannot and must not continue to be orientated predominantly to the *risk* of an accident, but must concentrate on the *damage*, more particularly on a “residual damage”, identical to a tolerable upper limit for damage $C \leq C_{\text{limit}}$. “Residual risk” has to be replaced by

“Residual damage”. Damage limitation is feasible reliably only if implemented deterministically by using passive means, with material barriers in the form of structural safety containments.

With this philosophy the safety objective can be defined in precise terms as “The entire impact caused by accidents must remain restricted to the inside of the safety containment, to protect human life and the environment from harmful releases”. That is our answer to the question “How safe is safe enough?” in dealing with hazardous materials and processes.

Because of their robustness, concrete components have to form the integral part used in any barrier. Thanks to wall thickness, heat capacity and tension softening, they are extremely resistant to impacts, shocks and penetrations, as well as fire and cryogenic attacks – to name just some of the effects involved in accidents.

If tightness requirements are prevailing the residual damage, the structural integrity is inadequate and the full integrity, including tightness, of the barrier must be guaranteed. Tightness is best defined in terms of a tolerable leakage rate. Concrete is properly tight, but problems may be caused by cracks, in particular separation cracks. Cracks can be avoided or their depth restricted if we prestress concrete. In this way tightness can be influenced and controlled with regard to quality and quantity almost at will and is then almost reliable. Coatings or linings are needed if this is not sufficient, for example if the uncracked or partly cracked concrete is too permeable for the substance affecting it. The integrity of these sealing layers is then normally dependent on the degree of prestressing. The criterion for this is once more the state of the cracks.

We will not, of course, rely only on passive safety, but combine it with active forms, so that both complement each other.

I would like to thank the members of the Working Group, specially the Chairman, Dr. Klaas van Breugel, for this work, dealing successfully with an outstanding subject in a very efficient manner. Being committed engineers and scientists the group accepted the challenge to write this important report, important for society and industry as well, to open up new ways to a sustainable development of our world. Part 2 of the report is somewhat drafted, Part 3 just roughly structured. I wish and I hope that the Working Group, now under the new leadership of fib, will be able to bring both parts to the end with engagement, competence and success.

Munich, December 1998

Helmut Bomhard
Chairman FIP Commission 8,
The Commission on “Concrete and Environment”

Preface

The enormous growth in scale and complexity of modern industrial facilities, and the associated increase in consumption of energy and raw materials, has put the environment under pressure. Pressure in terms of depletion of basic resources and of safety. Large-scale industrial accidents and severe pollution of the biosphere, as well as detailed analyses of hazard scenarios, have revealed the need for reconsidering currently used safety concepts. Among the many aspects involved in such a process of reconsideration, the protection of the environment is one of the important issues.

This report is the first of a series of three reports on structural protective systems against hazards. This first report deals with the nature and extent of the problem. Currently used safety concepts are briefly mentioned and evaluated. A survey of hazards and hazard scenarios further illustrates the weak points in traditional solutions. This evaluation reveals that the adoption of concrete structures can substantially enhance the safety of people and of the environment. Some examples of concrete protective structures are presented, showing the potentialities of concrete structures for reliable protection.

The second report of this series will deal with design tools for the structural engineer who is in charge for designing protective structures. These design tools may refer to either hazard actions, the materials behaviour and / or the structural response. In the third report examples of concrete protective systems will be presented in more detail.

The material for this report has been brought together by a small group of experts from the chemical and the building industry, consultants, authorities and the academic world. The input of individual members consisted of active participation in meetings of the working group and corresponding membership. The working group was part of the former FIP Commission 8 "Concrete Storage Vessel Systems". After the merger of FIP and CEB in May 1998, the work has been and will continue in the framework of *fib* Commission 3 "Environmental Aspects of Design and Construction".

Delft, October 1999

Klaas van Breugel
Chairman Working Group on
Concrete Protective Systems

1 Introduction

1.1 The Environment in Danger

In recent decades industrial activities and industrial facilities have shown an enormous growth, both in scale and complexity. This growth is accompanied by a large increase in energy consumption and use of raw materials, an increase in production of consumer goods and waste as a by-product. Storage and processing of raw materials and energy carriers often take place in large quantities in extensive facilities.

The size and complexity of modern facilities make them more and more non-transparent and difficult to survey. This makes these facilities susceptible to trouble, which may result in heavy damage in case of an accident. Although scale and complexity are not a problem *per se*, the combination with storage and processing of ever-larger quantities and concentrations of potentially dangerous substances constitute a technical, social and environmental hazard. A hazard is de-fined here, in line with Blockey [21], as "*a set of conditions in the operation of a product or system, with the potential for initiating an accident sequence*".

Well-performed risk and consequence analyses have evidenced the gravity of the present situation. Even more convincing than these analyses is the impressive list of past industrial and man-made environmental catastrophes. More than ever before it is recognised that the consequences of industrial activities, industrial catastrophes and environmental problems are border-crossing and even exhibit global dimensions. Large areas of fertile land have been converted into vast contaminated territories, inaccessible for man on penalty of health problems. There is no doubt any more: *The environment is in danger!*

Faced with these problems the question arises if, and how, structural engineering can contribute to solve, or at least alleviate, these problems. In order to answer this question we first have to concentrate on the nature and the extent of today and prognosticated problems.

1.2 Picturing the problem

Consumption of energy and raw materials

The majority of present problems is closely related to the increasing use of energy and raw materials. Since the population of the world and the consumption of energy and raw materials per capita is forecasted still to increase drastically in coming decades, it is to be expected that the hazard potential will increase as well. Statistics is quite convincing in this respect. Figure 1.1 shows the increase in energy consumption in past and coming decades.

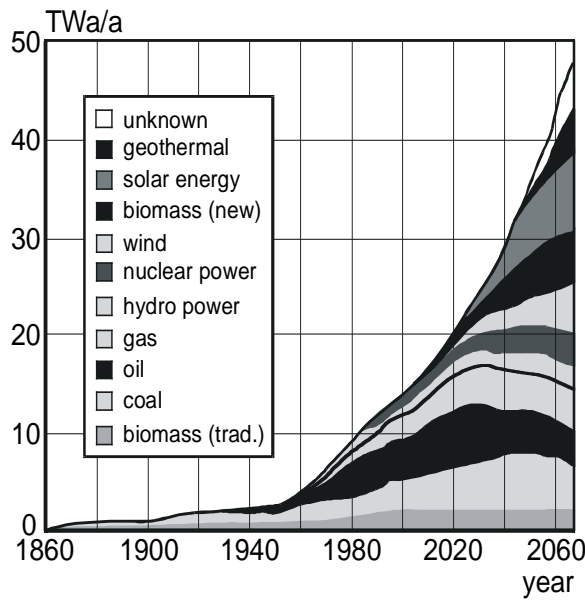


Fig. 1.1 Energy scenarios after different authors [1]

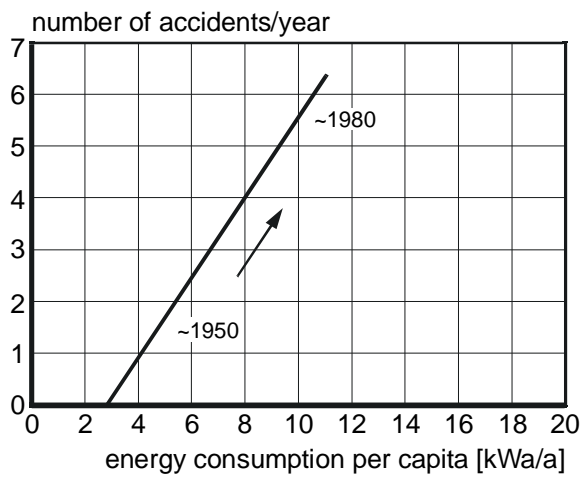


Fig. 1.2 Major industrial catastrophes as a function of energy consumption. Period '54-'84, (based on data in [20])

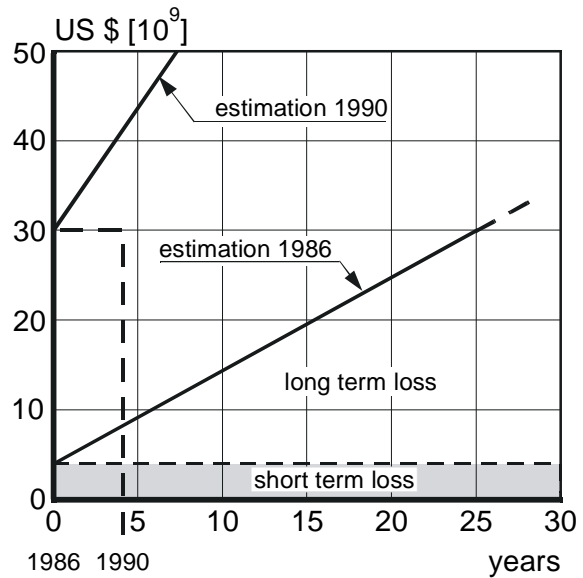


Fig. 1.3 Estimated direct and long-term losses Of the Chernobyl disaster. Estimates from 1986 [19] and 1990

For the reference period from 1954 to 1984, Fig. 1.2 shows the correlation between energy consumption and the number of industrial accidents per year with *direct* losses exceeding \$ 10,000,000. In many accidents this amount was exceeded by a factor of ten or even more. The direct losses in the Mexico LPG

disaster in 1984, for example, amounted to over \$ 150,000,000. Figure 1.2 also teaches us that, in spite of increasing awareness of industrial and technological risks, the growing investments in safety systems in recent decades have at best been enough to compensate for the increased probability of large accidents associated with the increased scale and complexity of modern industrial facilities. For a declining relationship between energy consumption and accident frequency either higher investments per unit of energy are required or more effective safety concepts have to be developed.

Indirect and long-term losses are generally much higher than the direct losses. This can be shown convincingly by referring to the losses experienced in the Chernobyl disaster.

An indication of the losses caused by this catastrophe is given in Fig. 1.3. The direct losses were estimated at 4 to 5 billion US dollars. Indirect and long-term losses due to deprived income from lost crops have been estimated at ten and twenty billion US-dollars after ten and twenty years, respectively [8]. In these figures claims for losses experienced outside the former USSR have not been taken into account. These losses also exclude the costs for extra health care for those who still suffer from the consequences of this accident, including the care for recently born disabled children. More recent figures show, that four years after the accident the losses have already reached the level that was expected after 25 years!

Catastrophes like the Chernobyl disaster and the nuclear accident in Harrisburg are examples of accidents, which, because of the huge and multi-disciplinary consequences, require special judgement. This issue is discussed in more detail in Chapter 2.

Costs for preservation of the environment

Huge amount of money is required to protect and clean contaminated soil and ground water. The costs of environmental damage in West Germany and the costs for cleaning of contaminated sites in the The Netherlands have been estimated at about \$ 100 10^9 [4] and \$ 30 10^9 [19], respectively. Related to a total population in these two countries of about ninety million people, the costs for rehabilitation amount to about \$ 1,400/ capita. Based on an energy consumption in these countries of 6 kW/a per capita, the costs per unit of energy consumed would be more than \$ 230/kW/a. The energy consumption in 1990 is, world wide, 11 TW/a. Assuming the energy consumption to be an indicator for the present pollution potential, the total costs for cleaning of soil and ground water would be $11 \cdot 10^9 \cdot 230 = \$ 2.5 \cdot 10^{12}$. This amount can be considered as a rough indication of the amount required for preservation of the environment and is in relatively good agreement with the amount of \$ 0.8 10^{12} mentioned by the World Watch Institute [2]. A substantial portion of resources needed for rehabilitation and preservation of the environment will be converted to civil engineering projects. In this respect the upgrading and building of large sewage systems, building of storage systems for intractable hazardous wastes, catch basins for fire fighting water, structural provisions for protection of soil and ground water against leakage of hydrocarbons at petrol stations and scrapyards and storage systems for various types of intractable hazardous wastes can be mentioned.

In almost all cases investing money in measures for protecting life and limb will in the end reveal to have been economically justified. The tremendously high costs for rehabilitation of the environment make it easy to believe this to be true. Apart from the question whether money spent on protective measures is economically justified or not, it must be considered just a matter of responsible stewardship to convert money, knowledge and technology to preservation of the environment.

Insurability of risks

The financial consequences of large natural or man-made catastrophes may be so high, that these financial burdens have to be taken by insurance companies. If sufficient statistical data exists, quantitative risk assessment will be the basis for the premium these companies have to charge so that they will not run into financial problems themselves. When statistical data is scanty, however, as it is the case with so called Low Probability/High Consequence Risks, a basis for probability-based decision making becomes too uncertain to rely on. It is particularly in these cases, that for the insurance industry a risk is primarily considered a financial threat. In case an accident occurs they must be able to pay for the maximum loss, however small the probability of occurrence would have been estimated [34]. It is for this reason, that the insurance industry emphasises the control of consequences rather than the control of risks or the probability of occurrence of an accident. Moreover, when a variety of non-financial risk aspects are to be considered, like economic, social, political, psychological and environmental aspects, insuring of risks becomes very complicated, if not impossible. Here we touch upon the limits of what has been indicated with responsible stewardship or responsible care.

Multi-Disciplinarity

There is no doubt that something has to be done to escape from the vicious circle leading to further destruction of the environment. All scenarios that have been worked out recently clearly demonstrate that solutions of modern environmental and safety problems require a *multi-disciplinary* approach. Just as it must be judged *incorrect* and *unfair* to hold one single discipline responsible for the contemporary problems, it would be unfair to *expect* comprehensive solutions from one single discipline. Reversely, it must also be judged *unrealistic* if one particular discipline would *claim* to have all-embracing solutions. Such a claim would only illustrate that the complexity and nature of environmental and safety problems have not been understood in full depth.

1.3 Solutions

Technical-fix approach

It has been stated that the present safety and environmental problems can be solved by a rigorous implementation of more technique and technology. This *technical-fix approach* presupposes that the nature of the problem is a technical, one-dimensional one. Instead of more traditional techniques, which may be more sophisticated, alternative methods would be needed, ending in perhaps an industrial revolution [35]. Against the background of the fact that today problems are predominantly technique-related, the technical-fix approach is still to be considered an untested hypothesis.

Revolution of the industrialised society

Instead of emphasising the potential of technique and technology as the most promising remedy for solving the problems of our industrialised society, we also find people who strongly support the need for a fundamental *change of mentality*. No longer the economic imperative of growth, but a re-evaluation and redefining of goals and norms for our society should be placed in the focus of attention. This change of mentality is not considered as the precondition for the realisation of an *industrial revolution*, but for a *revolution of the industrialised society*. By putting it in this way it is emphasised that the problems of the industrialised world can be solved neither by marginal changes of society nor by a major industrial revolution, nor even by the search for high-tech solutions of present problems, but the *cause* of all these problems should be in the focus of attention. A thorough search for the cause of many safety and environmental problems reveals that it is not the shortcomings of technique and technology, but rather its successes that have caused them.

An important implication for the present generation of engineers inferred from the forgoing is, that not merely high-tech trouble shooting, but comprehensive judgement of our technical and technological achievements should be made to his key-duties. It is clear that such a comprehensive judgement is impossible without addressing people's world view [28]. Since worldviews may differ quite substantially, the convergence of ideas, the formulation of goals and norms and defining criteria will not be easy. One can judge this a problem, but also as a major challenge of our decade.

The nature of the present problems requires the participation of a variety of disciplines, including the engineering discipline, in the discussion about the future of our society. The present generation of engineers should prepare themselves for their part in this discussion. It has to be admitted that, generally speaking, engineers are familiar primarily with technical issues. It is an inherent part of the required mentality change of our society, however, that engineers provide themselves not only with tools for solving technical problems, but also with an attitude to look first to the cause of the problems and concentrate on possibilities to anticipate them.

The drastic consequences of large-scale industrial catastrophes and the increasing flow of information on the detrimental effects of the use of fossil energy carriers on the climate (green-house effect) and the pollution of the environment have had a huge and negative impact on the appreciation of modern techniques and technology by society. Meanwhile everybody seems convinced that something has to be done to protect the environment and to guarantee safety of life and limb. It is the aim of this report to contribute to the interdisciplinary discussion on how to deal with severe risks in a modern industrialised society. This will be done by explaining the potentialities of protective systems for containment of large industrial catastrophes and for protecting the environment.

1.4 Protective structures

The focus of attention when considering different solutions to solve the safety problem will be on the potential of *concrete protective structures* as part of a comprehensive safety strategy. Reasons for focusing on concrete as a superior material for the design of protective systems will be dealt with in detail in Chapter 2. In anticipation of that more detailed argumentation it is noticed here already that:

- Concrete structures can be designed so as to resist a variety of extreme loading conditions like *impacts, fires, cryo-shocks, gas cloud explosions, airplane crashes* and *earthquakes*;
- A well-considered combination of concrete with reinforcing and prestressing steel enables not only a *robust* and *rigid* design, but also *ductile* structures with high *energy absorption capacity*.
- With addition of *admixtures, extra fines* and different types of *steel* and *synthetic fibres*, concrete can be tailored so as to fulfil the most stringent requirements deterministically, even tightness criteria.

By adjusting the shell thickness and thanks to the heat capacity, cold toughness and the softening behaviour when loaded in tension, concrete protective structures are resistant to heavy impact, perforation and thermal actions. It is these features of concrete structures, which make them unsurpassed for reliable *consequence control*. Why control of consequences is considered to be so important will be explained in the next chapter of this report.

2 Safety Concepts

The role of structural protective systems

2.1 Safety Concepts

In early primitive cultures people built structures to protect themselves. Protection was needed against the climate, extreme natural phenomena like tornadoes and floods and against wild animals. In a modern industrialised society things have changed drastically. The need for protection still exists. However, the objects which need protection are different. It is not merely people who need protection, but to an increasing extent also their industrial investments. Moreover, the hazards which have to be envisaged seem to be of another nature than before. The more people have intervened in natural and ecological systems and have tried to manage nature at will, the more this man-made environment appeared to change into a source of hazards. People have created their own enemy. They have to protect themselves against the man-made environment, the product of their own brains and activities. Moreover, they have to protect the natural environment against catastrophic pollution and deterioration processes caused by failing industrial processes and human errors. It can be concluded that people have to be protected against the consequences of both natural phenomena and the modern way of life.

Discussions on whether the advantages of an industrialised society really counterbalance the inherent disadvantages, generally concentrate on a *comparison of risks*. This *risk concept* has gained a lot of support in recent decades. Based on statistical accident data and accident scenarios, complex processes can be analysed and the weak points of complex systems can be traced in the design stage already. Large industrial catastrophes and increasing environmental problems have revealed, however, that a complete reconsideration of the risk concept is needed. Such a reconsideration is needed in all those cases, where the event probabilities can not be checked because of a lack of statistical data and where the consequences of an accident may become extremely high. Moreover, also from a more fundamental, philosophical point of view the risk concept requires a critical re-appraisal [4,6,7]. Particularly since licensing and approval authorities seem to be prepared to tune acceptance criteria for risk-bearing activities to the outcome of Quantitative Risk Analysis (QRA's). This development has raised a stream of criticism, partly maybe based without ground but partly on good reasons. To understand the reason for criticism, some basic features of the risk concept will be briefly discussed here. The evaluation of the risk concept automatically leads to the questions "How safe is safe enough" and "Are there realistic alternatives?"

2.2 The risk concept

The principle

First techniques for risk assessment date back to the 1930s and 1940s. Early applications of the risk concept are found in the insurance business. In the structural field first applications are found in aviation engineering [31].

In the traditional risk concept the risk R is defined as the product of the event probability $P\{F\}$ and the consequences C of that event. In formula form:

$$R = P\{F\} * C$$

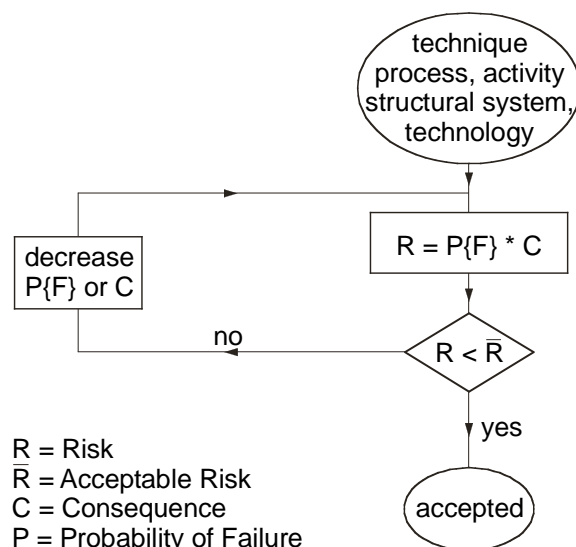


Fig. 2.1 Flow chart for decision making according to the conventional risk concept

The probability of failure depends on the density functions of both the available resistance and the actions. The consequences can be expressed in the number of fatalities or in financial losses. By dividing the consequences, i.e. the number of fatalities per year, by the number of people living within the sphere of influence of the risk-bearing activities, the individual risk (per person per year) is obtained. For judging the acceptability of risk bearing activities the calculated risk R is compared with a risk criterion. This criterion has to be defined by an owner or by legislative authorities.

Objectives

With the introduction of the risk concept it was aimed, and claimed, to have an *objective* and *rational* tool for decision making. There is no doubt that the risk concept, and implicitly the Quantitative Risk Analysis (QRA), is a powerful tool for *ranking of safety levels* and *tracing the vulnerable points* of structures, systems, facilities, processes and activities. At the same time, however, the risk concept has been judged inappropriate for *comprehensive* judgement of risk-bearing industrial activities [4,8,9]. This would hold particularly in case of Low Probability/High Consequence Risks. In those cases the theoretical risks are rather uncertain because of the lack of statistical data concerning magnitude and character of the actions. The results of risk analyses are, therefore, considered to be of limited use in decision making processes [22].

Residual risk

For risks below a certain small value the term "residual risk" has been introduced. A residual risk is the small theoretical risk that had to be accepted simply because of the fact that a zero-risk is not attainable within the framework of the risk concept. The residual risk principle, however, does in no way contribute to the control of consequences in case an accident occurs. On the contrary, it may free the way to justify and accept the introduction or continuation of risk bearing activities or processes, which should have been judged unacceptable if the activity in view would have been subjected to an integral judgement process in which all consequence aspects would have been taken into account [8]. In essence, a one-dimensional risk criterion, like a residual individual risk, has not the *quality* so as to make it an adequate parameter for judging risk bearing activities, techniques and technologies Integrally and comprehensively [53, 94]. Instead of judging against a one-dimensional criterion, a multi-dimensional approach has to be considered. This multi-dimensional approach is shown schematically in Fig. 2.2 as an Extended Risk Concept.

According to the diagram in this figure the single-valued acceptance criterion is now a sufficient criterion for *rejecting* an activity. At the same time it is an *insufficient* criterion for accepting an activity. For acceptance an integral, multi-disciplinary judgement of all *consequences aspects* is required. All the consequence aspects together form the *potential of disruption*. When this potential of disruption exceeds the limits of responsible stewardship, the activity, technique of technology should be rejected, at least in its unrevised form. The limits of responsible stewardship are not one-dimensional, but reflect the total set of norms adopted by society.

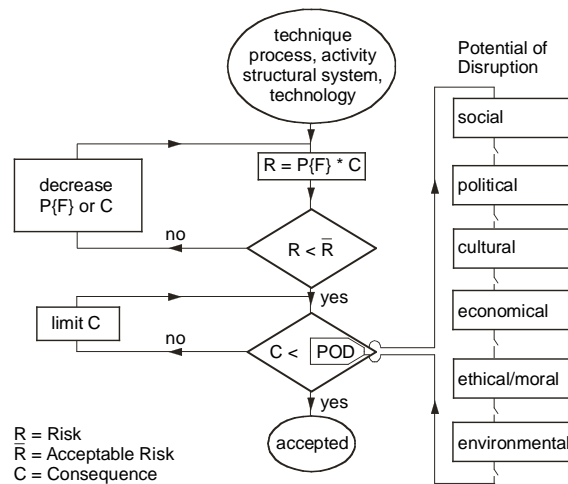


Fig. 2.2 Schematic representation of the Extended Risk Concept [94]

Accuracy and reliability of event probability

The calculation of the event probability $P\{F\}$ requires distribution functions of both the *actions* and the *resistance*. Of primary importance is, moreover, the consistency and the completeness of the *hazard scenarios* that are considered [12,13]. In the reliability scheme of Fig. 2.3 it is indicated that, going down from resistance via the actions to hazard scenarios, the uncertainty increases. This particularly holds for Low Probability/High Consequence Risks, in which case statistical data about hazardous loads is generally missing or at least too small for reliable predictions. This holds for technique- and technology-related data, as well as for the contribution of human error to the resulting theoretical risk.

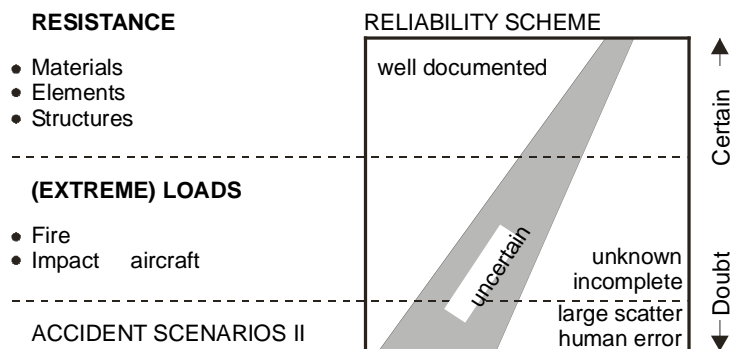


Fig. 2.3 Reliability scheme. Illustration of "degree of uncertainty" in different elements of theoretical risk and hazard analyses [10]

Judgement of theoretical event probabilities

Discussions are still going on as to whether a theoretical event probability must be considered as a *relative event frequency* or a *"degree of belief"* [14,21]. In case of low probability events, where statistical data is too little to verify the theoretical event probability, the theoretically obtained risk figures are interpreted as a degree of belief. If, however, a theoretical risk may not be assigned a frequentistic nature, one has to explain how this risk, i.e. this degree of belief, relates to events which are expected to occur in the real world, i.e. in space and time. Moreover, the question has to be answered whether a comparison of a degree of belief, having no frequentistic meaning, with a risk criterion that *does have* a hard statistical basis, is justified. Either one should compare quantities of the same nature or one shall refrain from comparing! If small figures do not tell anything about the probability of an event to occur somewhere and at a certain time in our real world, then it will become very hard to use these figures for convincing people about their safety. It must be born in mind that a change in terminology does not change the nature of figures. Based on the (in-)completeness and (in-)accuracy of the input, theoretical risk figures will be more or less accurate. But still these figures give information about events, which may occur in space and time. If due to a lack of statistical data the accuracy of a calculated event probability is very low, then this uncertainty should be made explicit instead of changing to another terminology.

A change of terminology does not solve any safety problem, but rather confuses the decision process. What finally counts is, that the probability of occurrence is not equal to zero. This implies that we have to consider the consequences of the event under consideration anyhow [29]. For a worthwhile discussion on the very subject reference is made to [23].

The acceptance criterion

In the risk concept a theoretical risk is compared with a risk which is considered acceptable to society. An accepted risk could be, for example, the individual risk that a person may die due to a "natural" cause at an age of fourteen. In the industrialised countries this risk is about 10^{-4} per year. Following the British Advisory Committee on Major Hazards [33], the acceptance criterion can be fixed at 1 per cent of this value, i.e. 10^{-6} p.a. (see also [33]). This is about one order of magnitude lower than the individual risk in traffic of 10^{-5} p.a. A risk of 10^{-8} could be considered negligible [32].

Whether it is justified to consider a *single valued* criterion, i.e. a fatality rate, as a *sufficient* criterion for judgement of risk-bearing activities is still a point of debate. Another point of concern is a more ethical point, viz. whether it is justified to take a fatality rate *unequal* to zero, even if it is a very low value, as an acceptance criterion for risk bearing activities. The ethical point is that, in essence, people judge themselves qualified to set the price, in terms of a number of fatalities, for the preservation of a certain level of prosperity *without* giving an answer to the question as to whether the present level of prosperity is justified at all!

"Zero times Infinity"

With increasing consequences C of an accident the theoretical probability of failure P{F} required to meet a specified risk criterion must decrease. This brings us close to a "zero times infinity" problem. This product is undefined and brings us beyond our experience horizon [7]. Any comparison of theoretical risks, of which the reliability can not be checked because that would take too long a verification period, with a statistics-based hard risk criterion, is debatable. Faced with this situation, alternative concepts have to be considered.

Valuation of non-material damages

A single-valued risk criterion, like an individual risk, obviously ignores the fact that the consequences of an accident are generally multi-dimensional [9]. The consequences of large accidents may be border-crossing and may affect economic and political relationships, cultural values, societal relationships, etc. Evaluating these non-material losses is a notorious problem. Actually we do not have a universally accepted format to value these effects.

Risk spectra

The foregoing remarks and objections can be explained with the risk spectra shown in Fig. 2.4 [4,11].

The risk spectrum K_1 indicates well-defined risks associated with, for example, storage of some raw materials and well defined industrial processes. Spectrum K_2 represents the risk adopted in some branches of the process industry, where catastrophic accidents have turned out to be possible. Examples are the Bhopal accident in 1986 [24] and the Mexico City LPG-disaster in 1984 [25]. Spectrum K_3 stands for activities of which the consequences in case of an accident are so high, or the probability even unpredictable, that it would not be justified to accept them. Examples of K_3 -risks are found in the waste management business, where either the long-term consequences in case of a failing containment are unpredictable. In order to cope with this type of problems "System Technology" has been introduced. Features of this system technology will be discussed in section 2.5.

Spectrum K_4 represents a Low Probability/High Consequence Risk. In those cases the theoretical event probability is so low, that no statistical data is available to verify these figures.

Core melt-down accidents in nuclear power stations are examples of these K_4 -events. In those cases we are extrapolating beyond our *experience horizon*.

For activities or processes, of which the risks fall in the right bottom corner of Fig. 2.3, the results of quantitative risk analyses become very uncertain. In these cases control of consequences is indispensable. Minimising the theoretical risks would only be speculative!

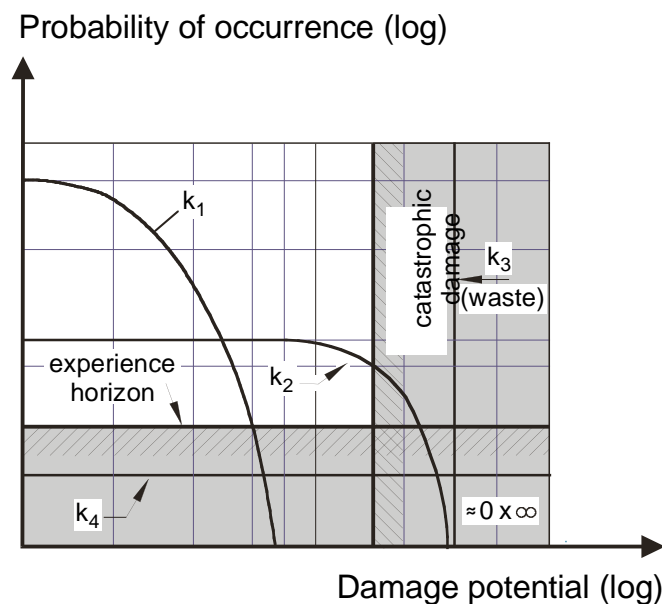


Fig. 2.4 Risk spectra (after [11])

2.3 Consequence Control

The consequence control concept

Unlike the risk concept, which is strongly probabilistic-oriented and focuses on limitation of the product of event probability and consequence, the consequence control concept is more deterministic-oriented and focuses primarily on the limitation of the consequences.

In this concept maximum credible actions, or loadings, are defined for which structural protective systems have to be designed deterministically, *irrespective* of the probability of occurrence of these loads. The maximum credible loads follow from well-considered accident scenario's. This concept is to be followed in all those cases where catastrophic consequences of an accident are conceivable.

The finite energy concept

A concept that, similarly to the consequence control concept, focuses on the control of consequence is the so called "Finite Energy Concept". Although not presented in the wording Finite Energy Concept, the basic principle of this approach has been explained by Eibl during the FIP-symposium in Budapest [7]. The idea behind the concept is that a product, whether it is identified as a raw material, an energy carrier or a waste, represents a finite amount of energy or a finite contaminating potential. The consequences of an accident with these products must, therefore, also be finite and can, in principle, be designed for with finite measures. Examples of this principle are the maximum fire duration of an LNG-fire, the maximum pressure in a nuclear containment in case of a major internal accident and the maximum blast overpressure caused by an explosion of a gas cloud of a certain volume. The maximum values of the actions are based on physical laws and have, in that sense, a deterministic character.

2.4 Safety-promoting methods

Once a certain safety level is defined, either in terms of an acceptable risk or acceptable consequences, several methods are available to realise these target safety levels. Traditional safety promoting methods are shown on the reliability scale in Fig. 2.5.

Active safety

Active safety deals with mechanical and electrical equipment, installed with the intention to avoid the occurrence of serious accidents. Active safety also comprises the regulations of a plant in operation and training programs to ensure that all the employees act according to the prevailing instructions.

For maintenance of many mechanical and electrical safety devices, operational tests and - if necessary - readjustments of them are to be carried out after fixed working periods. The level of active safety is endangered by adjustment aberration almost constantly. Furthermore it has been proved by experience that sometimes active safety devices have been put out of use in case they might affect the normal plant operation. It is obvious that in those cases it is a lack of discipline and human error rather than malfunctioning of the active safety devices that has to be blamed.

The active safety approach can be effective in all those cases where a clear understanding exists of things that *can* go wrong. It is well recognised, however, that major catastrophes are generally triggered by an *unexpected* or *incredible* chain of events. The Chernobyl accident, for example, resulted from a combination of events of which the coincidence had been assumed unrealistic [15].

A coincidence of events which goes beyond our logic or imagination cannot be anticipated, since we don't have a format according to which we should act in order to prevent the occurrence of a chain of events of which the coincidence had never been considered before.

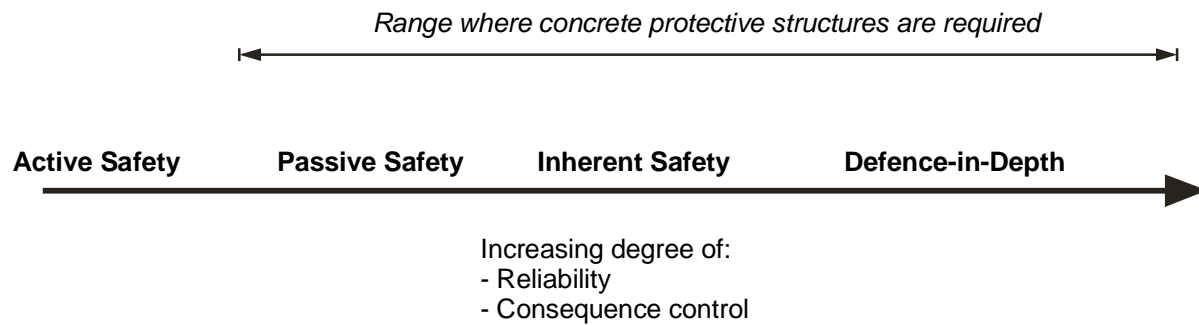


Fig. 2.5 Reliability scale (after [9])

Passive safety

Passive safety refers to structural systems, which are able to cope with the effects of accidental actions in such a way that the consequences remain limited. For their functioning, passive safety systems rely predominantly on natural laws and are almost completely *independent* of human intervention. Examples are the well-known fire wall and concrete safety walls and safety tanks around storage tanks for hazardous products.

Concrete structures, because of their robustness and massness, are very much suited to be designed as passive safety systems. Unlike active safety measures, there is hardly any chance for jeopardising the protective potential of a concrete structure due to human acts. Defects will evidence themselves directly after erection and can easily be repaired.

Inherent safety

Inherent safety refers to natural laws and to the plant lay-out. Elements of the inherent safety principle are found in the aforementioned Finite Energy Concept and are, in a way, also present in passive safety elements.

In principle, the idea of inherent safety is the best one to assure an appropriate safety level. An example of inherent safety is the absolute elimination (deterministically) of the probability that a pipe or vessel will burst due to internal overpressure by using non-pressurised transport and storage systems. In practice the implementation of inherent safety may meet considerable technical and operational constraints. Furthermore, it is typical for large-scale plants, that even after being put into operation, there are many revisions in the planning of the plant. Corresponding to the complexity of these procedures, the probability of human errors is high and may jeopardise the safety of plants that were initially designed on the basis of the inherent safety principle.

Defence-in-depth

Defence-in-depth relates to a *multi-barrier concept* with a high degree of natural or man-made *redundancy*. The concept may comprise all types of afore mentioned safety elements. The defence-in-depth principle has been developed in order to achieve maximum safety of nuclear power plants. At present the principle is also adopted for non-nuclear risk-bearing activities, for example for LNG storage tanks located in the close vicinity of populated areas or airports and for other facilities with a high damage potential.

2.5 System technology

The concept

"System Technology" is a new safety promoting concept, which can be used in those cases where traditional concepts are bound to fail. In those traditional concepts it is presumed that processes or activities which have to be safeguarded are well understood. This, however, is not always the case. In those cases system technology is considered a reasonable, if not the only alternative. The system technology concept is characterised by its *system redundancy*. The built-in system redundancy will enable people to intervene in processes which are not completely understood or uncertain at the onset of the period for which a certain protective measure has to fulfil its protective function. System technology is considered indispensable, for example, in case of storage of hazardous wastes, of which the chemical and biological composition as well as the possible reactions between waste and containment can not be predicted reliably. Examples and details of the system technology concept are discussed in view of the waste problem in the next chapters.

System technology versus materials technology

In the traditional safety philosophy emphasis is mainly on materials technology. If mechanical actions have to be designed for, one has to choose a material with certain strength. Designing for chemical attacks forces us to choose a building material with an adequate chemical resistance. In those cases the reliability and safety mainly depends on *materials technology*. With *systems technology*, on the contrary, emphasis is on the performance of the protective system as a whole. This includes materials technology, but is mainly characterised by the ability to guarantee adequate protection even in case of local, materials-oriented, failures of the system.

Characteristics of system technology

Characteristic features for a system technology-oriented design are

- Inspectability
- Controllability
- Reparability
- Renewability

without interrupting operation. These four features are of great interest when dealing with storage of hazardous wastes. Storage systems for wastes of which the composition is not sufficiently known shall be so designed to allow regular inspection and control of the structure storing the waste. If these inspections reveal damage, repair and/or renewal of the structure should be possible. Repair and renewal should be possible without taking the system out of operation. Examples of how to realise this are presented in Chapter 5.

Typical for the system technology concept is the anticipation on the occurrence of unpredictable events by providing well-considered built-in redundancy of the protective system. This is the best strategy for reliable control of the consequences.

2.6 Structural protective systems

For control of consequences the use of *passive safety components* are most appropriate. A *component* is considered a part of a protective *system*. A component may consist of several *elements*, viz. beams, walls, etc. *At present structural protective systems with a high built-in passive safety potential are judged the most reliable and also technically achievable solutions for adequate protection of the environment and for personal safety*. Particular features of those systems will be discussed in the following paragraphs.