Risk Assessment in the Federal Republic of Germany

Ulrich Hauptmanns[1]

discussion paper No. 94 / November 1997

[1]Institut für Apparate- und Umwelttechnik, Fakultät für Maschinenbau, Universität Magdeburg

ISBN 3 - 932013 - 17 - 4

ISSN 0945 - 9553

table of contents

preface

Preface

One of the central issues in the controversial debate on energy systems is the evaluation of risks associated with different options for energy supply and demand. Models of risks evaluation help to promote a rational discussion about the criteria for judging the acceptability of energy options. These normative criteria should meet the test of intersubjective validity, i.e. they should be, at least in principle, agrreeable or acceptable to all affected parties. Any decision on acceptability is also a decision about the allocation of risks, because it determines the relationship between the costs for suffering the potential consequences of the remaining risks and the costs for risk reduction.

Any judgment on acceptable risk levels relies on explicit or implicit criteria to evaluate the appriopriateness of each risk evaluation model. Such a comparison of models for risk evaluation requires a selection of meta-criteria. We chose the following meta-criteria: efficiency, incentives for risk reduction, applicability / feasibility and distributive fairness. All models of risk evaluation have been analyzed and evaluated on the basis of these four meta-criteria. The purpose of the exercise has been to generate a comparative review of different evaluation models and to point out the relative advantages and disadvantages of each model according ot the meta-criteria.

In a democratic system a risk evaluation model may encounter support only if the interests of those who produce risks are equally important to the interests of those who suffer from these risks. Our starting point for analyzing risk evaluation models has therefore been the individual utility of both, the risk producers and the risk bearers. Individual utilities constitute the final yardstick for evaluating risk acceptability in an ideal world. The crucial question, however, is

how to aggregate individual utilities for collective decision making and how to include external effects. There are four basic models that promise at least a partial solution to the problem of collective decision making (see Fig. 1/ sorry Fig. 1 is not available at the moment).

The first basic model refers to governmental regulation. A governmental agency is given the mandate to determine an acceptable risk level. This level is binding for risk producers and risk bearers. From an economic perspective „risk“ is conceptualized as a public good that needs governmental intervention. This baisc model includes risk evaluation methods such as comparisons, quantitative or qualitative setting (Best Available Control Technology = BACT ; As Low As Reasonable Achievable = ALARA) and economic valuation (cost-effectiveness-analysis, cost-benefit-analysis, decision analysis).

The second basic model refers to methods by which acceptable risk levels are negotiated between risk producers and affected individuals. The role of governmental agencies is confined to determine the legal conditions for those negotiations and to assure that they take place in a fair setting. The participants of those negotiations tend to internalize risks by selecting a risk reduction and management strategy on which all affected parties can agree, in principle. If all affected parties are involved in the negotiations, external effects of imposing risks on third parties are effectively internalized. This model comes closest to the market approach to risk management. Beyond direct negotiations, liability law is used for ex-post compensation of potential victims. It can be based on two different principles: causality (weak or strong) or intent and negligence.

The third basic model refers to the elicitation of criteria by experts. This model can be combined with the governmental approach to risk regulation. The idea is that experts in various fields should be empowered to set standards or to define the threshholds between acceptable and non-acceptable risk levels. Instruments within this model include expert panels, Royal Commissions and similar propfessional councils. Formal procedures such as Delphi, Consensus Conferencing, or Meta Analysis are used to determine a collective judgment.

The fourth basic model builds upon discursive approaches to risk management. These models emphasize democratic decision making enhanced by competent knowledge input and fair

representation of social interests and values. Although there is some similarity to the market model of negotiation, the main idea is not to bargain between different interests, but to develop a common solution to the risk problems. This solution should be based to the exchange of arguments among the people who will be affected by the decision. Discursive methods include consensus conferences, citizen juris, citizen panels and similar forms.

Each of those solutions to risk evaluation has its advantages and disadvantages. The theoretical approaches to risk evaluation can be compared with the actual practice of risk regulation procedures in several countries. These procedures are described and analyzed in the following reports:

- **Energy risk evaluation in France** (Marc Poumadère, Ecole Normale Supérieure de Cachan, Claire Mays, Institut SYMLOG, Cachan), discussion paper No. 89

- **Risk Evaluation: Legal Requirements, Conceptual Foundations and Practical Experiences in Italy. Case Study of the Italian Energy Sector.** (Natascia Petringa), discussion paper No. 90

- **Risk Assessment in the Netherlands.** (Giampiero E.G. Beroggi, Tanja C. Abbas, John A. Stoop, Markus Aebi, Delft University of Technology), discussion paper No. 91

- **Risk evaluation in the United Kingdom: Legal requirements, Conceptual Foundations, and Practical Experiences with Special Emphasis on Energy Systems.** (Ragnar Löfstedt, University of Surrey, Guildford), discussion paper No. 92

- **Risk evaluation: Legal Requirements, Conceptual Foundations, and Practical Experiences in the United States.** (Dale Hattis, William S. Minkowitz, Clark University, Worcester, Mass.), discussion paper No. 93

- **Risk Assessment in the Federal Republic of Germany.** (Ulrich Hauptmanns, Universität Magdeburg), discussion paper No. 94

Each study describes the required legal and procedural processes for risk evaluation in each country with special emphasis on energy systems. The authors analyze the reasons and the philosophy behind the adopted procedures. Furthermore, each study documents the practical experiences with the present practice of risk evaluation and collects the critical remarks that have been published in the literature or that have been expressed to them in personal interviews. Finally, each study concludes with a critical evaluation and assessment of the legal requirements and the practical applications of risk evaluation.

The various reports convey an extensive insight into the theoretical foundations and practical experiences associated with risk evaluation procedures. All volumes together provide a substantial contribution to the ongoing debate about risk evaluation and harmonization of risk regulations within Europe and beyond.

Gerhard Pfister and Ortwin Renn, November 1997

1 Introduction

In order to treat the subject of risk assessment, a precise definition of the term is in place. This and a substantial part of the subsequent text draws heavily upon /1/.

In everyday language the notion of risk is related to venture, hazard or danger, that is, the possibility to incur damage. In this sense risk is defined here as a quantitative measure of hazard.

Before assessing a risk it must be clearly defined and described which of the many possible risks are of interest and are to be determined. In this context, the following questions are asked:

- Whose risk is to be assessed?

For every individual or social group (family, community, economic enterprise, nation, etc.) there exist various specific risks. When referring to a person we speak of individual risk, in the case of several people the terms collective, societal, group or public risk are used. With an economic enterprise the investment risk is considered.

- Which risk to a person or to the public is to be determined?

The risks may be of a very specific nature; for example, death due to lightning or risks occurring in a more narrowly defined context like "working in the household" , "car traffic", or "operation of power plants".

- For what period of time is the risk to be determined?

A person or group is exposed to a risk as long as the possibility exists of the damage in question occurring. Some possibilities exist permanently, others only at certain times of the day or seasons of the year or only during clearly defined activities, for example, during the take-off or landing of an aircraft.

Every possibility to suffer damage is a risk, if it is uncertain, whether it will become reality. Damage and uncertainty therefore are the two elements which determine a risk. If

the magnitude of damage and the uncertainty of its occurrence may be quantified, then a number may be assigned to the corresponding risk, the risk number. Frequently, this number refers to a certain period of exposure, for example, one year. It is then called "risk per year".

1.1 The element of "damage"

In order to obtain a numerical value for the damage, it must be measurable, that is to say, expressible in units of measure. In case of an accident causing fatalities, damage is measured by the number of persons killed. Damage to property, for instance due to a fire in a factory, is measured in monetary units. For some categories of damage it is difficult to define measuring units; for example, to the environment or for psychic harm. Damages which are described in terms of different measuring units belong to different damage categories. In general, they are not comparable. Table 1.1 shows a few examples of different damage categories and the corresponding measuring units.

Table 1.1: Examples of measuring units of damages

Type of damage	**Measuring unit**
Human death	Number of deaths
Health effects	Number of affected persons (e.g. injured persons)
Regions rendered uninhabitable	Surface area
Material damage (replaceable)	Monetary units

The extent of damage cannot always be determined exactly. This is true for events in the past whose precise description may imply problems of delineation, and in particular for the analytical modelling of events potentially causing damage. For example, it is not always possible to determine whether observed detrimental health effects had already existed previously or whether they were caused by the event under consideration. If a study requires the consequences of an explosion to be treated analytically, a model must be developed which is capable of describing the propagation of the pressure wave on the basis of chemical and physical laws and of accounting for such influential factors as local conditions and possibly existing obstacles. In general, with such a model the magnitude of damage can only be assessed approximately.

1.2 The element of "uncertainty"

Uncertainty is expressed by the question "What is the probability of occurrence of an event?" Thus, we speak of probability as the uncertainty expressed in numbers. In mathematics the concept of probability has been precisely defined.

An impossible event has the probability 0 and an event with absolute certainty the probability 1. A possible, yet uncertain, event has a probability between 0 and 1. The more probable the event, the closer is this number to 1.

Probabilities are often estimated using the so-called relative frequency. For example, the probability of falling ill from influenza in 1996 in Germany may be estimated from the ratio m/n, where m is the number of people in Germany affected by this disease in 1995 and n the number of people potentially affected, i.e. the entire population of Germany.

This estimate is uncertain and the uncertainty can be quantified by determining an interval (the so-called confidence interval), which contains the correct probability with a certain level of confidence.

If probabilities derived from observations are to be used for predictions, then uncertainties frequently arise because the conditions under which the observations were made do not exactly apply to the period of time for which the predictions are to be made, as is the case with the foregoing example.

Probability values in practical risk calculations are, in general, only estimates. So-called objective estimates are based on samples from the exact population, for which the probability estimate is to be made. However, if the estimate is based on samples from different populations or on information whose suitability may be questioned, then the estimates are called subjective. They are then based on the personal judgement that the possible differences between the population from which the sample is taken and the population for which the estimate is to be made do not significantly affect the estimated value. This kind of subjective probability estimate is, particularly, necessary for predictions. Consequently, we then speak of subjective confidence intervals and subjective confidence levels. Subjective estimates can provide reasonable values if the personal judgement involved is based on professional experience, that is, if it is a so-called "expert" judgement.

1.3 Combining magnitude of damage and probability to risk numbers

1.3.1 Individual risk

Let y_1, y_2,... be elements of a denumerable set of different magnitudes of damage per occurrence of an event belonging to a certain damage category, for example number of casualties, and $WS(y_i)$ the probabilities of their occurrence in the time interval under consideration. Then the individual risk caused by them is described by the risk number:

$$R^* = y_1\, WS(y_1) + y_2\, WS(y_2) + \ldots \qquad (1.1)$$

The number R* is an estimate of the risk if either the magnitudes of damage or their probabilities of occurrence or both are estimates. It coincides with the estimate of the mean individual probability of the event, if this can occur only once and if each occurrence can only cause a damage of magnitude 1.

Often the expected frequencies of occurrence $h(x_1)$, $h(x_2)$,... of events causing damage of magnitude x_1,x_2,... are used. Then, the risk number

$$R = x_1\, h(x_1) + x_2\, h(x_2) + \ldots \qquad (1.2)$$

indicates the expected damage per year. If the magnitudes of damage per event are independent of each other, identically distributed, and independent of the number of occurrences of the event, then the risk number can also be determined according to the relationship $R^* = \bar{h}\bar{x}$. Here, $\bar{x}$ is the expected average magnitude of damage per event, and h is the mean value of its expected annual frequency of occurrence.

If the risk resulting from all events in a specified context, like for example the operation of a nuclear power plant, is to be assessed, then the risk numbers are added if the events are mutually exclusive.

1.3.2 Collective risks for a specific category of damage

In principle, the collective risk equals the product of the number of exposed individuals in the group and of the individual risk. Vice versa, an estimate of the individual risk may be obtained if the es-timate of the collective risk is divided by the number of exposed individuals in the group.

Collective risks may be quantified using the arguments which led to the formulae (1.1) and (1.2) for the individual risk. Thus, for example, if the frequencies of occurrence of traffic accidents causing $x_1, x_2, \ldots$ fatalities in a country in the coming year were known, then the collective risk could be estimated according to relation (1.2).

Naturally we would not normally calculate the collective risk using this formula, because the number of traffic fatalities in any one year is already a useful estimate for the following year, within the achievable accuracy (cf. the above example of the probability of being affected by influenza).

However, if we have to estimate risk numbers of events which have rarely or never been observed, so that figures from the past alone do not allow one to predict risk satisfactorily, the risk number can only be determined according to the formulae of types (1.1) and (1.2). This will be explained in more detail in the next section.

1.4 Risk numbers for rare or unobserved events

In sections 1.1.1 to 1.1.3 it was described how to combine the magnitude of damage (for a damage category) and its frequency to yield a risk number. Formally this is expressed by the simple relationships (1.1) and (1.2). By using these relations the risk numbers for different magnitudes of damage and all conceivable ways of any damage occurring may be calculated. Naturally, all possible magnitudes of damage and their respective probabilities or frequencies of occurrence then have to be known. Unfortunately, this is normally not the case for rare events. In the following section we use simple examples to show how risk is quantified in such situations.

1.4.1 Risk estimates based on observations of the complementary event

If the probability of occurrence of a rare event is to be estimated, it is an advantage if the so-called complementary event has frequently been observed. Commercial aircraft make several million take-offs and landings every year. The event "no crash during take-off or landing" is complementary to the event " crash during take-off or landing". If we assume, for example, that at airport A there have been 10,000 commercial take-offs or landings without a single crash, and if we take the first 1,000 take-offs or landings as a random sample, then it does not contain the event "crash during take-off or landing". According to the classical methods of statistics we may then conclude that the probability of occurrence of the event "crash of a commercial aircraft at airport A" has an upper bound of 0.003 at a confidence level of 95 %. Hence the corresponding confidence interval contains the values between 0 and 0.003. If not only the first 1,000, but all 10,000 flight operations are used, then the upper 95 % bound of the same event is 0.0003.

In the same way we could use operating experience with commercial light water reactors to estimate upper expected frequency bounds for certain events like a core melt. From 8,000 reactor years (experience with light water moderated reactors with a power of 400 MWe and more in the Western world) with the occurrence of one core melt accident (partial core melt in TMI-2) we may conclude that the expected annual frequency of occurrence of that accident for each reactor of the above category lies below 0.0006 at a confidence level of 95%. This upper bound is determined as if we knew absolutely nothing about reactors except for the fact that in 8,000 reactor years one such event has occurred. In contrast to the example of flight operations, no more observations are available to show that the upper bound is as high as it is only because of the relatively small number of observed reactor years. But even if a smaller upper bound could be estimated on the basis of additional observations of the complementary event, no statement could be made about the second element of the risk number, namely about the damage potentially caused by the event.

In such cases the events in question are decomposed into sub-events. This is done to a degree of detail such that

- partial events can be distinguished according to their influence on the magnitude of damage

and

- sub-events of these partial events can be recognized, which can lead to the partial event only in combination with other sub-events and their probabilities can be reasonably estimated from observations and additional knowledge of details

1.4.2 Risk estimates based on knowledge of details

Figure 1.1 outlines a risk assessment based on detailed knowledge proceeding from a description of the event to the determination of the damage and the risk numbers.

The outline can be divided into four steps:

a) "Event sequences"

All events contributing to the risk must be described in detail. This is done using event sequence diagrams in combination with fault trees (cf. chapter 3). The various event sequences consist of concatenations of sub-events A_1, A_2, ..., I_1,I_2,..., respectively which describe the failure or functioning of technical systems. They are characterized by

- their expected frequencies $h(T_i)$;
- the description of event characteristics (detailed characterization of the disturbance, i.e. cause, location, substances involved, etc.)

Fig. 1.1. Schematic diagram of a risk assessment based on detailed knowledge of event and exposition sequences

b) "Characteristics"

In this step the results of the different event sequences are described. This is done in terms of the components of the event characteristics which are essential to assess the damage (e.g. intensity of a possible explosion, level of heat and smoke generation etc.), which are quantified using experimental observations or model calculations.

Depending on the range of values of these components and their significance to an assessment of the damage, the results are divided for the sake of simplification into classes or categories k_1,k_2,.... These categories are characterized by:

- representative values of the components of the event characteristic as needed to assess the damage, and
- the sums of the expected frequencies of mutually exclusive event sequences from (a), which are assigned to the respective categories according to their characteristic. If, for example, category k_1 contains only event sequences T_1, T_2, and T_5 then for its expected frequency $h(k_1)$ we have

$$h(k_1) = h(T_1) + h(T_2) + h(T_5) \tag{1.3}$$

c) "Exposure sequences"

In this step all processes are described according to time, location, intensity and probability (exposure sequences $E_1,...,E_n$) through which the event characteristic could have a detrimental effect on the person or group of persons in question. The description must contain:

- the propagation of damaging components of the event characteristic, e.g. smoke in case of fire in accordance with the prevailing local conditions, M;
- the local distributions of the persons exposed to the risk, B;
- protective actions and countermeasures (evacuation, fire fighting, etc.), G.

In addition, probability estimates are needed for the different possible values of the components of M, B, and G. The arbitrarily large set of possible exposure sequences is thus approximated by a finite number of sets of discrete values (m,b,g). The probability of an exposure sequence similar to the specific local conditions, m (e.g. weather conditions during exposure), the specific exposure distribution, b, and the specific protective actions and countermeasures, g, thus becomes

$$W = w(m)\, w(b/m)\, w(g/mb) \tag{1.4}$$

In eq.(1.4) w(b/m) is the conditional probability for the occurrence of b under the condition m, and w(g/mb) that for the occurrence of g under the condition of the simultaneous occurrence of m and b.

d) "Damage and risk"

In this step the relation between the intensity of the damaging effects and all damages resulting from them is described. Hence for each set of values v = (category k, local conditions m, distribution of exposed persons b, emergency and countermeasures g) it must provide an estimated value x(v,a) of the magnitude of damage for each category.

Thus, using the estimate of the expected annual frequency

$$h(v) = h(k)\, w(m/k)\, w(b/km)\, w(g/kmb) \qquad (1.5)$$

the contribution R(v,a) of the set of values v to the risk number is estimated as the product of the expected magnitude of damage and its expected frequency of occurrence

$$R(v,a) = x(v,a)\, h(v) \qquad (1.6)$$

The estimate of the risk number for the category of damage in question, a, is the sum of the risk contributions R(v,a) taken over all considered sets of values v. It is therefore calculated according to

$$R(a) = S\ R(v,a) = x_1\ H(x_1) + x_2\ H(x_2) + \ldots \quad (1.7)$$

In formula (1.7) $H(x_i)$ is the sum of frequencies of those sets of values, v, which cause an estimated magnitude of damage x_i.

1.4.3 Uncertainties in risk assessments based on detailed knowledge

Results of risk estimates are in part based on parameters and relations which are not exactly known. A distinction has to be made between uncertainties due to

- random variations of parameters;
- inaccurate knowledge.

Uncertainties due to random variations form part of the risk to be determined because of their stochastic nature (e.g. different weather conditions).

Uncertainties arise from inaccurate knowledge of quantities like probabilities, expected frequencies, or parameters of physical models which are fixed or considered to be so during the period of time under investigation. In addition, functional laws can often be described only approximately or an approximation is deliberately used. This is particularly true for physical laws, like for example the dependence of conductivity of heat for gases upon temperature and pressure, but also for relations described by random laws using probability distributions. Such uncertainties are contained in risk estimates based on detailed knowledge.

Variations in the result for the risk due to random variations of the parameters are inherent; they cannot be reduced by improving the methods of analysis. On the other hand, uncertainties due to inaccurate knowledge can be reduced by improving the state of knowledge.

The aforementioned uncertainties can occur in all steps of a risk assessment.

1.5 Presentation of estimated risk numbers

The basic elements of the risk number are the magnitude of damage and the frequency with which a damage of this magnitude and of the category in question is to be expected during the time interval under consideration (mostly one year). In principle, it is sufficient to present the risk number together with the subjective confidence interval, if

-only magnitudes of damage 0 or 1 are possible (e.g. for the individual risk of the damage category "loss of human life"), or

-the magnitudes of damage per event are not too different and the event occurs frequently.

However, the requisites for the type of presentation are different if the risk numbers contain contributions from rare events with potentially large magnitudes of damage-. Thus, the risk number "0.01 per year" means, for example, that, averaged over the various possibilities during one year, the magnitude of damage per year is 0.01. This number can result from

- 99 possibilities with magnitude of damage 0 and 1 possibility with magnitude of damage 1, or from

- 999,999 possibilities with magnitude of damage 0 and 1 possibility with magnitude of damage 10,000.

If the possibility to suffer damage exists only during the next 100 years, the risk number 0.01 per year states, in the first case, that damage of magnitude 1 is to be expected during this period of time. In the second case, however, it is meaningless to speak of expected damage of magnitude 1, because there will either be no damage (probability = 0.9999), or

damage of magnitude 10,000 (probability = 0.0001) within these 100 years. For this reason risks from rare events with large potential magnitudes of damage are described by both the magnitude of damage per year and its probability of occurrence (respectively, magnitude of damage per event and its expected annual frequency of occurrence). Additionally, the risk number is also given. As a rule, risk is stated as the probability that the magnitude of damage per year exceeds some given value X*, respectively that the expected annual frequency of damage has a magnitude $X \geq X^*$. For example, in the case of the frequencies all expected frequencies of risk contributions with magnitudes of damage $X \geq X^*$ have to be summed. This summation is already included in the representation of risk by means of the so-called complementary cumulative distribution function (CCDF), which is called complementary, because it gives the expected frequency for $X \geq X^*$, whereas the probability distribution gives that for $X < X^*$. Thus, for a given value X*, the complementary probability distribution answers the question: "What is the expected annual frequency of damage of magnitude $\geq X^*$?"

Figure 1.2 shows a complementary cumulative distribution function. Additionally, subjective

Fig. 1.2. Complementary cumulative distribution function (CCDF) with subjective confidence interval

confidence intervals are given for the different risk contributions. They form an intuitively clear band about the determined complementary probability distribution. This band is the subjective confidence interval of the curve and it states:

"The propagation of the quantified uncertainties through the steps in Fig.1.1 indicates, that the correct curve lies somewhere in the region between both limiting curves, at P% subjective confidence level, provided the influence of the non-quantified uncertainties is negligible".

An interval of analoguous meaning can also be given for the risk number.

The separate representation of the risk for the different damage categories, for example, early and late fatalities, makes it impossible to trace which magnitudes of damage of the different categories stem from a set of values v from section 1.4.2, i.e. which of them have been caused by the same event sequence. Such relationships would have to be illustrated for the different sets of values by using tables.

1.6 Problems of delineation

It is important to define clearly the scope of the risk analysis. For example, in the case of nuclear power plants, the risk resulting from normal operation and that from accidents has to be distinguished. It must be made clear whether the operation of the power plant alone or the entire fuel cycle are to be investigated. For other types of electricity generation, for example the use of solar energy, risk contributions from accidents are generally small. However, the risk resulting from the construction of the plant may be significant due to extensive construction work and the large volume of construction materials. In the case of process plants it is important to define whether the chemical process as such, or also transport and storage of the required substances are to be

considered. The distinction between the risk from normal operation and that from accidents is also important for this type of plant. A further question to be considered besides the risk resulting from the utilization of an energy source or of a chemical process could be the risk of insufficient supply resulting from its non-use.

If different technologies are to be compared, the time of reference is also important. Since the risk of a technology also depends on its degree of maturity, the question arises whether all investigated systems should be judged on the basis of their technical development level at an identical point in time or if credit should be given to less developed technologies for a possible improvement of safety in the future. This is particularly important, because, in general, risk comparisons are made with regard to future decisions. These few examples may suffice to demonstrate the necessity of a neat delineation.

1.7 Generalities on probabilistic methods for safety and risk valuation

Frequently, the risk of complex technical systems cannot be derived directly from statistical observations; its estimation requires a probabilistic risk analysis, which has as its objective to assess the damages caused by accidents and their expected frequencies of occurrence.

As already explained in section 1.4.2, such analyses are based on the identification of representative sets of conceivable accident sequences and the determination of their effects. For this purpose models of the technical systems and their components are developed and analysed. Accident sequences in plant systems are normally represented by event sequence diagrams (event trees), which in a simple way describe the potential effects of accident-initiating events depending on the functioning or failure of the safety

systems required for their control. The probabilities of failure of these systems are estimated by fault tree analyses. The use of these probabilities in the event trees then permits the estimation of the expected frequencies of occurrence of the damage-causing event sequences. Further investigations are made to determine the loads on additional safety devices and their potential failure modes; for example, the failure of containments and the quantities of dangerous substances which would then be released. The resulting damages are calculated with models describing the transport of dangerous substances and their effects on man and environment. Owing to their analytical procedure, probabilistic reliability and safety analyses account for the interactions of all important design features and operating conditions as well as the environment.

The scope of risk analyses can vary. It can be divided into three levels:

Level 1: Analysis of the operating and safety systems of the plant.

Level 2: In addition to the analysis of level 1, potential loads on containments of the plant are assessed.

Level 3: In addition to the investigations of level 2, the consequences of accidents are determined.

A level 1 study mainly consists of a reliability analysis of the operating and safety systems and of their modes of operation. Its objective is to identify accident sequences leading to potentially dangerous processes in the plant. At the same time the major causes of such sequences and their expected frequencies of occurrence are established. The investigation comprises the step "event sequences" shown in Fig. 1.1. The analyses allow

one to judge whether the safety level of the technical plant systems, their design and modes of operation are adequate for avoiding dangerous processes inside the plant.

Additionally, in a level 2 analysis loads on containments caused by dangerous processes and their failure modes are determined. These are obtained from the corresponding investigations of the plant systems. Results are modes and times of failures of barriers, types and quantities of released dangerous substances or energy, and the expected frequencies of such occurrences. They provide certain insights into the risk of the plant.

Additionally, in a level 3 analysis the transport of dangerous substances and energy in the environment of the plant is investigated. Resulting consequences and their expected frequencies of occurrence are assessed. Hence, the results of the plant systems analysis are combined with the analysis of dangerous processes inside the plant up to the destruction of containments. These, in turn, are coupled with the results of accident consequence calculations. Thus, a comprehensive appraisal of the risk of a plant becomes possible.

Analyses of levels 1 and 2 would nowadays be called probabilistic safety analysis (PSA) because they do not address potential consequences of accidents; only a study of level 3 would be a probabilistic risk analysis (PRA)

2 Application of risk analyses in Germany

In what follows a short account is given of the legal background of the application of risk analysis and probabilistic safety assessment in Germany.

2.1 Nuclear energy

On the basis of the constitution of the Federal Republic of Germany and the Atomic Energy Act /2/ nuclear power plants are generally licensable, even if this implies accepting certain risks. In order to guarantee ample protection against the dangers of nuclear energy the Atomic Energy Act subjects the use of nuclear fuel and other radioactive materials to complete control and supervision by government authorities. The licensing requirements are formulated as a set of rules of prohibition with the proviso of permission, contrary to other areas of technology. Accordingly, a nuclear power plant can be licensed only, if the necessary provisions are made according to the state of science and technology against damage caused by the erection or operation of the plant.

The notion of necessary provisions requires interpretation and concretisation. The purpose of this norm is the protection against hazards; according to it hazard is assumed in situations in which the uncontrolled progression of events may lead to damage with a sufficiently large probability. In this context, sufficiently large probability does not imply a fixed numerical value. The degree of uncertainty of occurrence of the damage, i.e. its probability of occurrence, must be judged according to the necessity of protection of the endangered rights and property and the magnitude of damage. If the magnitude of damage can be very large, already the remote probability of its occurrence would be sufficient to assume danger. In view of possibly catastrophic consequences of nuclear accidents the application of the atomic legislation assumes danger already for accidents with very low probabilities of occurrence. This interpretation of the notion of danger

corresponds to the principle of adequacy which has the rank of a constitutional law. Because of the potentially very large consequences events even less likely than those considered in the context of adequate protection of the individual have to be accounted for to protect the public /3/.

The demonstration of adequate protection of the individual and the public from danger is an indispensable requirement for licensing. In particular, a license must be denied if the plant may cause damage which violates rights or property of the individual, which are protected by the constitution. The individual whose rights or property are affected, is entitled to an actionable claim of sufficient protection.

The distinction between the two areas of provision, protection from hazards and precautions against risks can be interpreted as follows:

'Protection from danger' comprises all provisions which are required for the protection from danger, in particular to the rights and property of the individual independently of expense and technical realizability. The potentially affected individual is entitled to an actionable claim.

'Best possible protection from danger' describes the obligation of the authorities to examine the necessity of provisions against damage and their adequacy on the basis of the best available information, namely according to the state of science and technology.

'Precaution against risk' goes beyond the protection of the rights and property of the individual from danger and comprises provisions for mitigating impacts or reducing the frequencies of occurrence and consequences of events capable of causing damage. Provisions against risk below this level of hazard may be demanded in the process of appraisal, or in many cases because of legal ordinances derived from /2/. The individual is not legally entitled to claim specific precautions against risk.

'Best possible precautions against risk' describes the execution of dutiful judgement which accounts for all important objectives. For example, the differing requirements for the protection of the population, the environment, and employees, and for achieving operational safety have to be balanced against the benefit to the economy, and the

prospects of development of nuclear technology. Conflicts of objectives have to be resolved as far as possible. The principle of adequacy of cost and benefit has to be taken into account. The dutiful execution of judgement is subjected to judicial control in case of disputes.

"Only the continuous adaptation of the circumstances relevant for risk evaluation to the most recent state of knowledge can satisfy the principle of best possible protection from danger and precautions against risk " /4/.

The method of probabilistic safety analysis represents the current state of science and technology. Consequently, probabilistic safety assessment has to be used for safety relevant decisions to the extent appropriate for the protection according to the Atomic Energy Act. Decisions on safety which disregard the use of probabilistic safety analysis without sufficient justification would be faulty.

For this reason the elaboration of probabilistic analyses is called for in the Safety Criteria for nuclear Power Plants /5/. Criterion 1.1 “Basic Principles of the Provisions for Safety” contains the general requirement to demonstrate that nuclear power plants are sufficiently safe. Concerning the methodology it states that the assessment of the balancedness of the safety concept, which is based on deterministic procedures, is to be supplemented by assessing the reliability of safety relevant systems and parts of the plant using probabilistic methods as far as this is possible according to the state of science and technology with the required accuracy.

This made the Reactor Safety Commission decide that probabilistic safety analyses have to be carried out in the context of the recurrent safety appraisals of power plants in operation /6/. These analyses have to be updated taking into account operating experience, abnormal occurrences and results from reactor safety research. The procedure to be adopted is outlined in the PSA-Guideline /7/ which was published in 1990. Several supplements to this Guideline are in existence; however, they have not yet been ratified.

The Guideline requires level 1+ studies to be performed, which in addition to level 1 analyses cover a safety assessment of the active functions of the containment isolation system..

2.2 Chemical plants

There is no ruling concerning the application of probabilistic analyses for the safety assessment of chemical plants in Germany. Hence, the assessment is entirely deterministic granting the licensee the right to operate his plant if he demonstrates that erection and operation comply with the relevant laws and, in particular, correspond to the state of technology. The second administrative prescription of the Incident Ordinance /8/ enumerates the methods for safety assessment and indicates that the use of fault tree analysis (cf. section 3.1.4.2), the pricipal tool of probabilistic analyses is possible. However, it is not mandatory. Instead frequently a qualitative method of safety analysis, the so-called Hazard and Operability Study (HAZOP) /9/ is used in order to demonstrate plant safety.

However, the COMAH-Directive (Seveso 2) of the European Community /10/ issued in December 1996 may bring about changes as to the relevance of probabilistic methods for the safety assessment of chemical plants in Germany.

2.3 Aircraft industry

Based on the European Regulation JAA 25 (para 1309) failure probabilities have to be assessed for all systems of an aircraft. Details are given in the corresponding ACJs (advisory circulars). In addition, operating experience is evaluated in a procedure

involving administration, air -transport companies, and aircraft manufacturers in order to update the studies performed in the course of the licensing procedure and to improve safety.

3 Methodology

The total risk of a process for energy production comprises the risk of the conversion process, a possibly required fuel cycle, and the risk derived from the construction of the plants and from the acquisition of the necessary materials. Similarly in chemical plants the risks from the process, storage, transportation and final disposal of substances as well as those derived from the construction and the acquisition of the necessary materials have to be considered.

In the case of aircrafts, which contrary to the two types of stationary systems addressed before are mobile systems, chiefly the risk from operation has to be accounted for.

As explained in Chapter 1, the assessment of any risk of mass phenomena, for example, from occupational or transport accidents, is based on statistical evaluations of records on the past; for rare events, like the core melt in a nuclear reactor, analytical methods are used. Damage to health as a consequence of emissions is estimated by epidemiological investigations and extrapolations from higher to lower doses. In calculating the risk contributions from the installation of plants two different methods are used: process analysis and input-output analysis.

In a process analysis the most important materials for building the plant are identified and their necessary quantities are calculated. Drawing upon statistics for the industrial branches concerned, the risk caused by their production is assessed. This is augmented by the risks from accidents during the transport of the building materials and the construction. The procedure is schematically shown in Fig. 3.1.

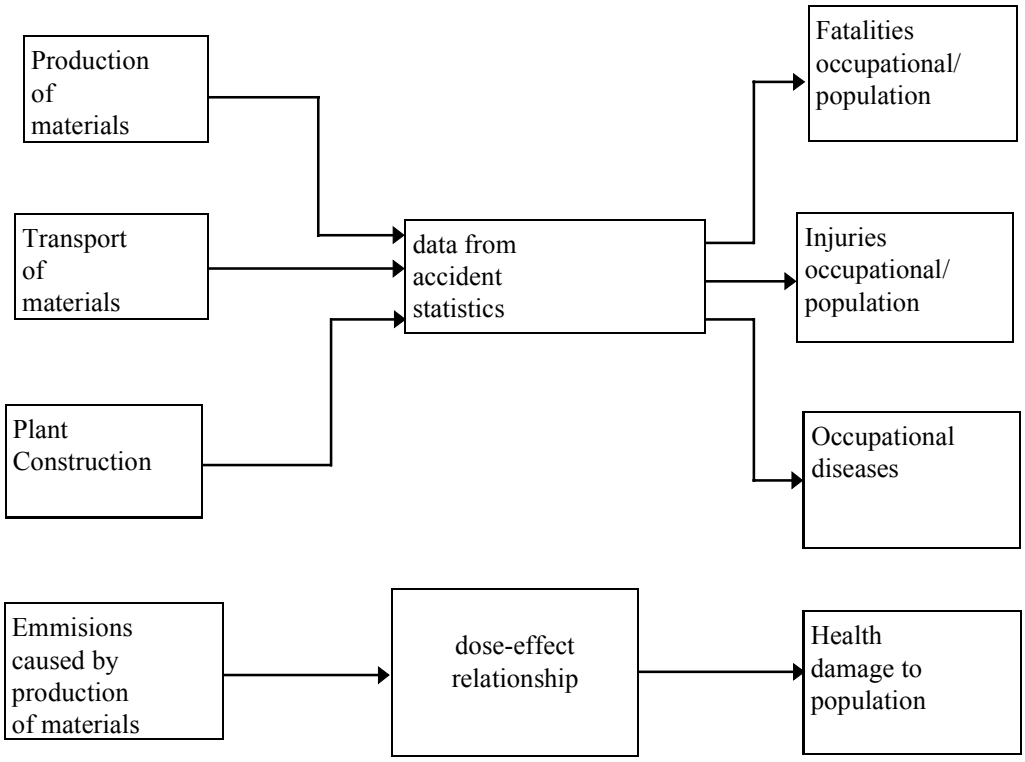

Fig. 3.1. Outline of the calculation of plant construction risks using a process analysis

In an input-output analysis the interactions of all segments of an economy are represented in the form of a matrix, as shown in the example of Table 3.1. The lines contain the sales of the respective segments to all others; the columns state the input of goods and services to one segment of the economy from all the other segments. In this way, all goods and services received from any of the segments of the economy are registered in monetary units. Using appropriate factors these may be converted into risk numbers; for example, accidents per unit quantity of product for the different segments of the economy.

Table 3.1. Example of an input-output table

Output / **Input**	**Agriculture and fishing**	**Ferrous metals**	**Non-metallic minerals**	**Construction**
Agriculture and fishing	0.076	0	0	0.008
Ferrous metals	0.006	0.305	0	0.152
Nonmetallic minerals	0.005	0.010	0.101	0.530
Construction	0.026	0.004	0.002	0

The application of the input-output analysis to the assessment of risks is outlined in Fig. 3.2, which shows the model developed by the Brookhaven National Laboratory (BNL) for the calculation of the environmental impact and health effects of different technologies. In this model the economy is divided into 110 segments. The advantage of using the input-output analysis stems from the fact that the contribution of the entire economy to the construction of a plant is accounted for. Therefore there is no need to determine which materials and activities contribute substantially to risk, as is required for process analysis.

Fig. 3.2. Outline of the Brookhaven National Laboratory (BNL) model for calculating environmental impacts and health effects

As a practical example for the difference between process analysis and input-output analysis figures are given which were obtained for deaths and injuries in the construction of windmills. If the contributions of the total economy (systemwide effects) are taken into account, the risk is estimated by a factor of two or three higher than if the analysis is limited to the directly used materials and the construction process of the plant. Further details are found in Table 3.2.

Table 3.2. Labour requirements and occupational accidents for generating 1.06 1015 J using windmills calculated according to the process and input-output analyses (preliminary values)

	Fatalities	**Illness**	**Labour**
	in 10^{-4}	**in 10^{-1}**	**in man-years**
Direct occupational impacts (process analysis)	78.5	55.	118
System-wide occupational impacts (input-output analysis)	171.0	196.0	243

Nevertheless, a limitation of both procedures is that all changes in the economy are assumed to be marginal. The activities of building the power station must not interfere with the economy so as to cause significant changes in the production and accident structure in the segments involved. However, this does not apply to major programmes for promoting certain energy systems. In such cases new production lines will have to be built and the figures from the past will no longer be applicable. A detailed analysis of the economy would then be required and the risk data to be used would have to be estimated by experts. This difficult situation is not yet treated.

The risk values required for performing the aforementioned investigations are inscribed into the two previously mentioned categories, that dealing with mass phenomena like transportation events and that concerned with rare events as, for example, nuclear-reactor accidents. Since the estimation of risk values for mass phenomena is relatively straightforward, the following sections are concerned with the calculation procedures to be adopted in the case of rare events.

Emphasis is placed on stationary plants. The expected damage of an aircraft crah is basically the death of passengers and crew. Further implications depend upon the location of the accident.

A complete risk analysis comprises five tasks, viz.:

1. Collection of the basic plant data.
2. Identification of initiating events.
3. Event sequence and reliability analyses.
4. Investigation of the release of dangerous substances and energy.
5. Assessment of the accident consequences.

In the first task basic information on the plant, the applied procedures, and the processes involved is collected. The following three tasks concern the investigation of potentially dangerous processes inside the plant including the possibility of damage to containments or of their destruction. In the fifth task the transport of dangerous substances in the environment or the environmental impact of energy and the resulting detrimental effects are investigated. The expected frequencies of occurrence of the event sequences thus considered are estimated.

3.1 Plant systems analyses

3.1.1 Collection of basic plant data

The basic plant data provide the fundamental information on the plant and the hazards potentially caused by its processes and operational procedures. They refer to the

- design of the plant and its systems,
- operating conditions and operational procedures,
- site of the plant and its surroundings.

In particular, data which are essential for the assessment of hazards are compiled, i.e. information on:

- dangerous substances,
- quantities of these substances and their distribution inside the plant,
- dangerous conditions of the plant,
- available safety and protection devices.

Details on the site and its surroundings are only required if a level 3 analysis is to be performed. Information about the plant comprises a description of the plant and its structure, and of the design and construction features of its systems and components. In addition, operating and handling procedures are described. For characterizing the site, information about the population distribution and the traffic situation in the vicinity of the plant and on the location of protection zones is needed.

3.1.2 Identification of initiating events

On the basis of the plant data, initiating events must be identified which potentially endanger the plant personnel and the population. It is useful to distinguish between plant internal and external events:

- examples of internal events are

  mechanical failures of active components (e.g. pumps) and of passive components (e.g. pipework or vessels);

  malfunctions or failures of measuring or control devices ;

  loss of energy and media supply;

  human error;

- examples of external events are

  natural phenomena like lightning, earthquakes and flooding;

  impacts from neighbouring industrial plants;

  impacts from means of transportation (e.g. aircraft crash or the explosion of a road tanker);

  sabotage.

It is impossible to analyse all conceivable initiating events in detail. Rather it is sufficient to deal with those which are essential, i.e. which are significant as to frequency of occurrence or magnitude of damage or both.

The expected frequencies of initiating events are generally derived from observation. They are either estimated directly from operating experience (e.g. electrical power grid failure) or the initiating event is broken down into sub-events for which operating experience is available; its frequency of occurrence is then calculated by a fault tree analysis (cf. /12/ and section 3.1.4.2). Apart from that there are cases where the frequency of occurrence is obtained from model calculations (e.g. large breaks of pipes of a nuclear reactor coolant circuit) or estimated by experts.

3.1.3 Event sequence analysis

In an event sequence analysis, starting from a defined initiating event (e.g. pipe break) and depending on the functional success or failure of the operating and safety systems required for coping with this, its different possible consequences are determined /13/. The paths of events resulting therefrom are combined in an event sequence diagram, also called event tree, as shown in Fig. 3.3.

Fig.3.3: Example of an event tree

By simulating the dynamic behaviour of the plant, the systems which have to function are identified along with those which have to be activated additionally in order to control the initiating event. The simulations are based on mathematical models of the physical or chemical processes involved. Each path of the event tree is the static description of a process which is continuous. This process is represented by a few points in time (junctions) at which, depending on the success (upward path in the diagram) or failure (downward path in the diagram) of the required systems, its further progression is determined.

For fixing the minimum success criteria of the system functions, i.e. the minimum number of systems and functions needed for coping with an initiating event, results from accident progression simulations are frequently used which were carried out for other purposes, e.g. reactor licensing.

The event sequence analysis consists of two sub-tasks, namely

- plant systems analyses concerning those aspects of the event sequence which are determined by the action of the operating and safety systems, and
- investigations of event sequences which lead to the release of dangerous substances and energy as a consequence of the failures of the operating and safety systems of the plant.

The event trees of the first sub-task contain all paths which proved significant in the plant dynamics investigations and because of their requirements on operating and safety systems. In general, the binary logic is used, that is, systems are either considered fully operative or totally failed. Possible intermediate states are assigned to one of the two states, usually the failed state. The second sub-task is only required for an analysis of level 2 or 3.

The following aspects are relevant for an event sequence analysis:

- dependencies between different system functions may exist, because countermeasures to an initiating event are frequently performed by systems which are not independent of one another. The requirements on the system functions normally depend on the event sequence in question and on the type of initiating event.
- secondary failures (see section 3.1.4.3) may occur as a consequence of previous system failures. The structure of the event sequences, that is, the chain of subsequent events, corresponds to the time history of the accident. Hence, when dealing with an event of the chain the consequences of earlier events must be considered. For example, if water

leaking from a pipe renders a measuring device or a safety system inoperative, then this would have to be accounted for in further analysis.

3.1.4 Reliability analysis

The evaluation of event trees requires numerical values for the reliabilities of the systems in order to assign probabilities to its paths. Observations which allow the reliability of the system to be estimated directly are usually not available, especially if failures are rare owing to high system reliability. However, the failure rates of components, which normally exist in larger numbers if several systems are taken as a basis, can be evaluated statistically. Parameters obtained in this way are the starting-point for estimating system reliabilities. Normally, components have several functions, for example, the opening and closing of a valve. Therefore, it must be determined which of its failure modes contributes to system failures. For this reason we often speak of the failure of a function or of a functional element instead of the failure of a component.

Besides the design of a system, its operational scheme must be taken into account in the reliability analysis. For example, emergency diesel generators are only started on demand; on the other hand, most cooling water systems are in permanent operation.

If a system function is required at a certain point in time, i.e. on demand, then the probability to be in a failed state at this instant is denominated "unavailability". If a system function must be maintained during a certain interval of time but this is not achieved, then we speak of "failure probability" or "unreliability". Often a combination of both is required, e.g. when an emergency cooling system is modelled. It must be available on demand and perform its function for a certain period of time. Unreliabilties and unavailabilities, respectively their complementary values to 1, are the probabilities assigned to the paths of the event trees (cf. Fig. 3.3).

3.1.4.1 Determination of failure probabilities and unavailabilities of components

In a probabilistic systems analysis component behaviour is described by failure probabilities and unavailabilities. Procedures and operator actions are treated like components. An independent functional element is assigned to each function of a component of the investigated system. A single functional element is also used for treating dependent failures of a certain function of several redundant components (cf. section 3.1.4.3).

The failure behaviour of a functional element can be described in one of the two ways

- by the failure rate l

  (the failure rate can be interpreted as the relative decrease of the number of unfailed functional elements which occurs in a unit of time).

– by a probability of failure on demand (unavailability) p

(the probability of failure on demand is the probability of failure of the functional element on demand, i.e. the probability of failure of the component function in the time interval prior to or at the instant of time of the demand).

Both quantities are derived from experience. They are estimated by evaluating statistically observations made during the operation of similar technical systems. Thus, mean values of the failure rate, l, or of the unavailability, p, are calculated from the failure behaviour of several similar components working in a comparable environment. In general, both parameters are not constant in time. This is subsequently explained for the failure rate,l., whose time history can frequently be described by a "bathtub curve", as shown in Fig.3.4.

Fig 3.4. Time history of failure rates

In the initial phase of operation so-called early failures may occur, e.g. due to latent design defects or quality or manufacturing deficiencies which have remained undetected despite quality assurance and burn-in tests. The number of faulty components decreases with increasing time of operation due to repair or replacement until only components of the same quality level remain. Towards the end of the component's life the failure rate may increase again due to wearout and aging. During the major part of the component's life its failure behaviour is nearly random, i.e. not determined by systematic failures. Therefore failure rates are taken as constant. In this case they are the reciprocal values of the mean lifetimes of the components. The random failures are described by an exponential function, i.e. the failure probability q(t) of a component as a function of time is given by

$$q(t) = 1 - \exp(-\lambda t) \tag{3.1}$$

The evaluation of operating experience generally provides time averaged values for the failure rates or failure probabilities. These constant values are used in the reliability analyses. They usually refer to independent failures of components. Since the body of observations of dependent failures is mostly small, specific analyses are necessary for estimating their influence, as explained in section 3.1.4.3. A special role is played by operator errors. The different acts to be considered have to be analysed in order to assign failure probabilities to them (cf. section 3.1.4.4). These are then used to quantify the "components" operator error in a fault tree.

Apart from the failure behaviour of components, their unavailability due to maintenance must be accounted for. Maintenance is understood here to include repair, replacement, and functional tests. From the moment of failure, respectively the start of the test, until the maintenance act is terminated the component is considered as failed. In the theoretical treatment of maintenance the following aspects play a role:

- the frequency of demands of the function, respectively, the time interval between regular functional tests (inspections) and their time staggering for failures which are not self-announcing;
- the assumption of immediate repair, as soon as the failure is noticed;
- the assignment of the "as good as new" property to the component when the repair is completed.

It may be necessary to consider several failure modes if several functions of a component are important for a system function. In such cases the fault tree analysis accounts for different failures of functional elements of a component. As an approximation, these failures are often assumed to be independent from one another.

Apart from repairs of components after a failure causing an operational disturbance, repairs of components for other reasons, e.g. failures with no immediate effect on operation, and replacements during preventive maintenance have to be accounted for. It may then be necessary to disconnect or dismount the component temporarily, in which case it cannot fulfil its function. If such maintenance work is carried out during the operation of the plant, the availability of the system function is reduced.

3.1.4.2 Fault tree analysis

Fault tree analysis is an established tool for analysing the reliability of complex technical systems. In such an analysis an undesired event (e.g. loss of coolant or release of dangerous substances) is defined. Then a search is made for all causes which may possibly lead to this. In general, a large variety of failure combinations of various components is obtained which make subsystems fail. The failure of a sub-system may either directly cause the undesired event or do so in combination with failures of other sub-systems or components. The combinations are described by logical "AND" and "OR" and occasionally "NOT" gates. The choice of the type of gate and the structure of the tree naturally reflects the underlying dynamic behaviour of the system in response to the initiating event, i.e. the time dependent physical and chemical processes occurring in it.

In fault tree analyses complex relations within systems are described using the binary logic, which considers only the functioning or failure of components. This, together with a suitable graphical presentation (cf. Fig. 1.1, where A_1 is the undesired event), permits a transparent and comprehensive treatment, even of very large technical systems. Specific problems like human error and dependent failures can be accounted for. The fault tree is the logical model of a technical process with regard to the undesired event.

Fault tree analysis is a complete procedure. Due to its deductive nature it yields all combinations of events leading to the undesired event, if it is consequently applied. Limitations are not inherent in the process of analysis but result from possible lack of

knowledge and care by the analyst. Obviously, a fault tree analysis cannot reveal phenomena which are unknown at the time of its execution.

Fault trees for complex technical systems can only be evaluated with computer programs.

3.1.4.3 Dependent failures

Besides independent failures of functions of components, dependent failures may occur.Their consequences may be particularly severe if they affect redundant components or sub-systems presenting themselves simultaneously or within a short interval of time such that the failed states coexist. Such failures were called common-mode failures (CMF) and cover different types of dependent failures which are outlined below:

- failures of two or more similar or identical redundant components or sub-systems due to a single shared cause. They are referred to as common cause failures (CCF);
- failures of two or more redundant components or sub-systems resulting from a single previous failure. They are called propagating or secondary failures;
- failures of two or more redundant components or sub-systems caused by functional dependencies, i.e. resulting directly from the structure of the system. For example, functional dependencies may result from a common auxiliary system (e.g. instrument air supply), from a common control device or from human error.

In order to adequately treat dependent failures in a reliability analysis, failures of components due to functional dependencies should be modelled in the fault trees. Propagating failures, as far as they cannot be excluded on grounds of spatial segregation or adequate design of the components, should also be modelled in the fault trees (e.g. secondary failures induced by missiles, by pipe whip or a hu-mid environment).

If this is done, there remain those dependent failures which are due to shared causes (CCF) (design, construction, or maintenance errors, e.g. unsuitable lubricants in pump bearings). If possible, these should be quantified on the basis of operating experience. Several types of failures have to be distinguished in this context:

- failures which can either occur or be detected only in case of an accident,
- failures detected on demand of a function (in functional tests or in other recurrent system demands),
- self-announcing failures.

Operating experience primarily provides data for the last two types of common cause failures, which are detected during the normal operation of the plant. Failures which occur or can be detected only during an accident must usually be predicted by analytical methods. The potential for such failures will, however, only remain undetected if operational requirements or routine functional tests are not representative for the requirements on components or systems under accident conditions.

The quantification of common cause failures detected during operation or functional tests is difficult, since observations are usually scarce. This may be explained as follows:

- only a small fraction of component failures are dependent failures;
- causes of system failures which have been detected are usually eliminated. Similar failures will then only recur with an even smaller probability.

If operating experience is not sufficient for the quantification of common cause failures, recourse is taken to models. Such models are described for example in /14/.

3.1.4.4 Human error

When quantifying human actions in reliability and risk analyses, man is regarded as part of the system, i.e. he is treated as a system component. He has to fulfil a certain task within a given interval of time. If he does not achieve this the "component man" is considered to have failed. Man is distinct from technical components in that his behaviour is characterized by a substantially larger variability and complexity. Therefore, the description of his behaviour in terms of reliability parameters is difficult. In particular, complex interdependent actions involving several persons or decision situations are hardly amenable to probabilistic treatment. Experts on human behaviour

therefore agree that only such actions or elements of actions can be described by reliability parameters which refer to skill or rule-based behaviour, as defined below.

Operator actions are classified into three categories

- rule-based actions (or behaviour). Behaviour in which a person follows remembered or written rules, e.g. performance of written post-diagnosis actions or calibrating an instrument or using a checklist to restore manual valves to their normal operating status after maintenance. Rule-based tasks are usually classified as step-by-step tasks unless the operators have to continually divide their attention among several such tasks without specific written cues each time they should shift attention to a different task. In the latter case, in which there is considerable reliance on memory, the overall combination may be classified as a dynamic task, especially in a post-accident condition.
- skill-based actions (or behaviour). The performance of more or less subconscious routines governed by stored patterns of behaviour, e.g. the performance of memorized immediate emergency actions following a loss-of-coolant accident or an initiating event, or the use of a hand tool by a person experienced with the tool. The distinction between skill-based actions and rulebased actions is often arbitrary, but is primarily in terms of the amount of conscious effort involved; in layman terms, the amount of "thinking" required.
- knowledge-based actions (or behaviour). Behaviour which requires one to plan one's actions based on the functional and physical properties of a system.

For the purpose of analysis actions pertaining to the first two areas of behaviour are broken down into single elements to a degree such that reliability parameters can be assigned to these elements. The best known and most widely used method for this is THERP (Technique for Human Error Rate Prediction) /15/.Other methods are reviewed in detail in /16/.

The THERP method can be divided into four steps:

1. Identification of those failure combinations which will make the system function under consideration fail, if human error is taken into account.

2. Identification and analysis of the human tasks related to the system function in question (task analysis).

3. Assignment or estimation of the relevant failure probabilities taking into account the specific conditions for the performance of the action by the so-called performance shaping factors (PSF). The basic human error probabilities of /15/ are multiplied by these factors, which are greater than 1.

4. Assessment of the influence of human error on the probability of failure combinations (composed of the failure of technical components and human error) and on the unavailability of the system function (as part of the reliability analysis).

Two elements of this method deserve special attention, the task analysis and the decomposition of a complex action into its constituents. The task analysis precedes the quantitative evaluation and implies a systematic identification of the parameters which affect human reliability. In performing the decomposition existing dependencies must be identified and accounted for.

Some problems have been pointed out for which there seems to be no satisfactory solution at present using neither THERP nor any other method. These are discussed below.

As already mentioned, suitable methods and data are available for "skill-based" and "rule-based" behaviour However, their applicability to knowledge-based behaviour is limited. Objections are made primarily by cognitive psychologists. They refer to the great complexity and variability of human behaviour, particularly if decisions have to be made in new and complicated situations. Other questions which still seem to be insufficiently covered are the quantification of dependencies between several subsequent steps of an action of a single operator, between joint actions of several operators, and of the control of the action of an operator by another person. The assumptions made in this context are still insufficiently supported by operating experience. Likewise the use of the so-called recovery factors for treating situations in which human error has no negative consequences because of "forgiving" properties of the system may be regarded as lacking.

In order to apply the procedures and data presented in /15/ to other, e.g. German nuclear power plants, an adaptation to the specific conditions is necessary. There may be differences in the technical design (e.g. degree and extent of automation), in the ergonomic design (e.g. use of mimic diagrams), and with regard to administrative and organizational measures (e.g. organization and training of the staff), which have to be accounted for.

3.1.5 Determination of releases of dangerous substances or energy

The release of dangerous substances or energy into the environment occurs only if their containments are damaged or destroyed. In general, the loads resulting from disturbed plant conditions have to be determined using mathematical models which describe complex physical and chemical phenomena. The probabilities of damage or destruction of barriers are derived from such calculations. In addition, particularly for chemical

plants, spontaneous failures, i.e. failures whose causes are not or cannot be determined, of storage or transport tanks under nominal conditions must be accounted for. Expected frequencies of such release mechanisms can be derived from operating experience. Furthermore, there exists the possibility that barriers are destroyed by external events, e.g. heating up by fire or as a consequence of shock waves from explosions.

The determination of the quantities of dangerous substances released from damaged containments usually requires the use of complex models. They must account for the possibility of chemical reactions and processes like condensation, evaporation, agglomeration and deposition, which may occur during a release. The quantities of released substances and the intensity of their detrimental effects may strongly depend on the time history of these processes.

The final results of the plant systems analysis are extent, location, time history, released energy, and expected frequencies of releases from the plant which potentially cause detrimental effects. Releases occurring in different accident sequences are often combined into sets of representative releases, the so-called release categories (cf. Fig. 1.1). These categories are characterized by:

- representative features for the determination of damage,e.g. quantity and type of released radioactive, toxic, flammable, or explosible substances as well as
- the sums of expected frequencies of mutually exclusive event sequences assigned to the category in question on the basis of its characteristics

By combining event sequences to categories the volume of the required accident consequence calculations can be substantially reduced.

3.2 Determination of accident consequences

3.2.1 Environmental transport

The extent of damage caused by a release of dangerous substances or energy depends, among other factors, on the type and quantity of the substances, and on their transport behaviour. Additionally, the dose-effect-relationships plays a role in case of radioactive or toxic substances and the combustibility or explosiveness for other dangerous materials.

The factors which influence the transport of a substance depend on the transport path. Most important are the air and water paths. However, the water path is often not considered in risk studies In case of atmospheric dispersion, the conditions close to the location of release (buildings, structure of the surface of the ground), the type of release (evaporation, buoyancy due to released energy), and the meteorological and topographic conditions are of importance.

During the dispersion process potential reductions of the quantity of dangerous substances by chemical reactions, radioactive decay, or dry and wet deposition have to be taken into account. For quantifying the risk, expected frequencies of meteorological situations, wind speeds, and precipitation in the surroundings of the plant have to be obtained.

If the released substances are flammable or explosible, the consequences of a release depend on whether, and at what distance from the location of release, ignitable mixtures are formed, and if ignition sources are present and ignition occurs. To assess the consequences, the variation of the concentration of the dangerous substance with the distance from the location of release and the probability of the presence of ignition sources at a given location have to be determined.

3.2.2 Calculation of release effects

In order to assess the effect of a dangerous substance the damage-causing mechanism has to be known. For example, the following categories of damage are considered: early fatalities, injuries, development of diseases (in particular cancer and genetic mutations),

detrimental environmental effects and economic losses. Dose-effect-relationships for toxic and radioactive materials and details of the pos-sible exposure paths of the substances like submersion, immersion, inhalation, or ingestion are necessary for quantification. In the case of explosions or fires, the effects of pressure and heat on people and property must be known.

The significance of an event is measured by the extent of damage to people and property. Damage to humans are death, injury or diseases which break out shortly after the event or in the long run. Damage to be expected in later generations due to genetic effects have to be included as well.

Damage to people can be quantified in terms of the number of fatalities, the number of injured, or the reduction of life expectancy. In order to determine this the population distribution in the surroundings of the plant is important; in case of long-term effects of dangerous substances calculated from dose-effect-relations without a threshold, the population distribution far away from the plant is also needed. Countermeasures like seeking shelter in buildings, evacuation, medical treatment, and the interdiction of contaminated food have also to be taken into account.

Among property damage the loss of agricultural products and of natural resources, destruction, the cost of relocating the population and of decontaminating affected areas have to be taken into account. This is quantified in terms of money or areas.

4 Experience to date with risk analysis

Considerable qualitative and quantitative insight accrues from determination of the risk of a nuclear power plant, much of which can be put into practice.

Qualitative insight stems from the identification of those plant components, protection and safety devices, and modes of operation which contribute to risk. The subsequent quantitative evaluation then shows the risk-dominant accident sequences. It also shows how risk is diminished if the frequencies of occurrence of such sequences are reduced. Such investigations are of prime interest when judging whether proposed measures for plant improvement are adequate and balanced. In plant-specific risk analyses, insight into peculiarities of plant design and modes of operation may be of interest even if they are not related to risk-dominant accident sequences.

Although large uncertainties still remain with risk analyses of nuclear installations, many useful results are obtained which are not solely derived from or are dependent upon the calculated numbers. For prac-tical purposes the most important result of a risk analysis is the comprehensive description and documentation of design characte-ristics, generated in the modelling of accident sequences. The determination of expected frequencies of accident sequences does not have to be more accurate than is required for distinguishing between risk-dominant and less important sequences. The insights into plant design and modes of operation can be taken into account in the licen-sing procedure. Further development of licensing requirements may benefit from them.

Determination of the relative importance of risk-dominant accident sequences allows cost-benefit analyses for potential plant modifications to be carried out, both with regard to increased plant safety and to a balanced design of the plant.

The models developed in risk analysis can be used to optimize test and maintenance intervals and to improve modes of operation and personnel training. Insights from

uncertainty analyses can help determine research priorities, particularly if large uncertainties are shown to exist in risk-dominant accident sequences.

Investigations of nuclear power plants have revealed that the essential contribution to severe environmental impact results from core destruction accidents and that the integrity of the containment is of great importance for the prevention and mitigation of offsite consequences.

The analyses have shown that the most important contributions to uncertainties in the results occur in the treatment of the following topics:

Level 1:

Treatment of common cause failures and human behaviour as well as the modelling of physical processes, particularly of thermohydraulic phenomena in emergency core cooling and transients.

Level 2:

Modelling of the physical phenomena during core destruction as well as modelling of physical and chemical phenomena associated with the trans-port and deposition of radioactive substances within the containment; determination of the time and mode of containment failure and the treatment of hydrogen explosions.

Level 3:

Selection of parameters for the atmospheric dispersion, the estimation of dry and wet deposition rates, of the thermal lift, and of the dose-effect relationship for early and late fatalities.

Frequently the uncertainties inspire new research programmes.

Risk studies reveal weaknesses of the plant design, and point to areas where the investment into safety is inadequately high. Possible risk contributions from inadequate operational procedures are also recognized. Relative contributions to risk can be estimated from the numerical results. Therefore improve-ments and modifications can be introduced where they are most effective.

The benefits of risk analysis may be be summarized as follows. It provides

- the topology of accident sequences;
- quantitative descriptions of damage-causing events and estimates of their expected frequencies of occurrence;
- the event sequences which contribute significantly to the risks;
- insights into the adequacy of plant design and operational modes by determining those plant components and modes of operation which contribute most to the expected frequencies of the risk dominating event sequences.

This provides the basis for judging

- the level of safety of a plant or a technical device;
- the safety relevance of new scientific and technological results or of specific incidents during plant operation;
- promising approaches for the improvement of safety.

The insights gained from reliability and risk analyses can be used in engineering for

- eliminating weaknesses, also at interfaces between systems;

- identifying additional possibilities for improving plant safety;
- achieving a balanced design with regard to safety;
- improving modes and specifications of operation;
- improving the training of operators;
- identifying parameters with significant influence on accident consequences;
- determining key research areas and research tasks.

4.1 Nuclear power plants

Probabilistic studies based on the German Guideline will be available for most German Nuclear Power Plants by the end of 1997. Those already submitted have been reviewed and basically led to two classes of recommandations for improvement, one of them to be realized in the short run, the other in the long run. Details may be found in /17/. It must be emphasized, however, thazt these studies are of level 1+, as mentioned in Chapter 2. That implies that in addition to the scope of a level 1 study the reliability of the active systems of the reactor containment is assessed. However, no estimate of possible consequences is made.

The only study of level 3 performed to date in Germany is the German Risk Study (Phase A) /18/

In the context of its execution or as consequence of its results of the German Risk Study Phase A system modifications were implemented in the reference plant, the Biblis B Nuclear Power Station. They are cited here as an example of the possible impact of probabilistic studies on safety. This is reflected in the resulta of the posterior Phase B of

the German Risk Study /19/, which are significantly influenced by the following modifications:

- installation of a semi-automatic system for the controlled,
- cooldown at a rate of 100 K/h in the case of small leaks,
- improvements of the relief valve station of the secondary circuit,
- automatic partial cooldown of the plant, if the main heat sink is not available,
- control of the pressurizer relief system through various additional isolation signals,
- possibility of restoring connection to the main grid in the case of a failure of the emergency diesels,
- installation of a backup grid connection.

Insights obtained in /18/ have led to numerous improvements of the plant design and to optimized maintenance strategies. For example, manual actions of the operating crew have been partially automatized (e.g. manual cool-down of the plant at the rate of 100 K/h in the case of small leaks in the primary coolant system). Also, the possibility of recovery of offsite power after a failure to start the emergency diesels was provided. All of this has led to a more balanced design of systems.

4.2 Process plants

A probabilistic study for process plants covering physical consequences but not the impact on the population has been performed for Liquid Gas /20/. In addition, a number of probabilistic safety analyses have been performed (cf. /21/, /22/) including one study addressing start-up and shut-down as well as normal production operation.

In all cases weaknesses of the technical systems and, in some cases, of the man-machine interface have been identified. On this basis, improvements of the design have been suggested and the potential benefits from their implementation have been calculated.

4.3 Aircraft industry

As mentioned in section 2.3, analyses of systems reliability are mandatory for the licensing of an aircraft type. The benefits of probabilistic analyses for the design of safe systems and of the feedback from operating experience are generally recognized.

5 Critical assessment of the risk assessment practice in Germany and proposals for improvement

The standardized procedure of demonstrating the achievement of reliability targets in the aircraft industry is fully acceptable and represents an important contribution to aircraft safety.

Probabilistic safety assessment, as performed in the nuclear industry in support of licence related matters is adequate. It implies that the study primarily aims at improving plant safety and is not performed under the imperative of demonstrating compliance with fixed numbers. The reason is, that complex analyses of this type should not be carried out under pressure, because -contrary to a mere reliability analysis- they leave a considerable margin of imterpretation..

Great emphasis is placed on the consideration of uncertainties, at least as far as studies in the nuclear industry are concerned. They constitute an important element of the process of taking decisions on the basis of study results.

Studies thus far carried out in Germany suffer from the drawback that they refer to isolated items as the plant or storage and not to the entire cycle involved. For example in order to assess the impact of a planned increase of exclusion areas around gas storage sites, it should be taken into account that a possible reduction of risk accompanying this measure is offset or outweighed by the fact that fewer storage sites will be available, which will lead to an increase of road and rail transport and the associated risk.

A wider use of risk assessment techniques will draw attention to physical and chemical phenomena underlying potential accidents which are not yet fully understood and their relevance. Thus they will have a positive impact .on directing research efforts to worthwhile topics.

6 References

/1/ Hauptmanns, U. and W. Werner: Engineering Risks - Evaluation and Valuation, Berlin 1990

/2/ Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz) vom 23. Dezember 1959 (BGBl. I, S. 814), in der Fassung der Neubekanntmachung vom 31. Oktober 1976.

/3/ Urteil des Verwaltungsgerichtshofs Baden-Württemberg, 30. März 1982 (Wyhl-Urteil) 575/77, 578/77, 583/77/

/4/ Beschluß des Bundesverfassungsgerichts, 8.8.1978 (Kalkar Beschluß), 2 BvL 8/77

/5/ BMI-Sicherheitskriterien für Kernkraftwerke vom 21. Oktober 1977

/6/ Empfehlung der RSK vom 23. November 1988, Abschlußbericht der Ergebnisse der Sicherheitsüberprüfung der Kernkraftwerke in der Bundesrepublik

/7/ PSA-Leitfaden, Facharbeitskreis “Probabilistische Sicherheitsanalyse für Kernkraftwerke”,Oktober 1990

/8/ Zweite Allgemeine Verwaltungsvorschrift zur Störfall-Verordnung, (2. StörfallVwV) vom 27. April 1982 (GMBl. 1982 S.205)

/9/ A Guide to Hazard and Operability Studies, Chemical Industry safety & Health Council of the Chemical Industries Association Ltd.London 1977

/10/ Council Directive 98/92/EC of 9 December 1996 on the control of major-accidents hazards involving dangerous substances, Official Journal of the European Communities, L 10, Vol. 40, Brussels, 14 January, 1997

/12/ Fehlerbaumanalyse - Methode und Bildzeichen - Teil 1.DIN-25424 (1981)

/13/ Ereignisablaufanalyse - Verfahren, graphische Symbole und Auswertung.DIN-25419 (1985)

/14/ Hauptmanns, U. , A. Kreuser und J. Peschke: Vorgehensweise bei der Behandlung von GVA, GRS-A-2160, Köln, Juli 1994

/15/ Swain, A.D.;Guttman, H.E.:Handbook of human reliability analysis with emphasis on nuclear power plant applications.NUREG/CR-1278, SAND80-0200 RX,AN (August 1983)

/16/ Swain, A.D.: Comparative evaluation of methods for human reliability analysis, GRS-71, Köln 1989

/17/ Spitzer, C.:Experiences from reviews of probabilistic safety assessments, Kerntechnik 60 (1995) No. 2-3, 99-104

/18/ Deutsche Risikostudie Kernkraftwerke. Eine Untersuchung zu dem durch Störfälle in Kernkraftwerken verursachten Risiko, Köln 1979

/19/ Der Bundesminister für Forschung und Technologie (Hrsg.): Deutsche Risikostudie Kernkraftwerke - Phase B. Köln, 1990 (English Summary: German risk study nuclear power plants, phase B.GRS-74, Köln 1990)

/20/ Bundesanstalt für Materialprüfung (BAM) (Hrsg.): Ermittlung sicherheitstechnischer Kriterien zur Flüssiggastechnologie und Herleitung geeigneter Sicherheitsstandards Förderkennzeichen des BMFT: 01 RG 8402, 1988

/21/ Hauptmanns, U. et al.: Ermittlung der Kriterien für die Anwendung systemanalytischer Methoden zur Durchführung von Sicherheitsanalysen für Chemieanlagen, GRS-59, Köln Dezember 1985

/22/ Hauptmanns, U. und J. Rodriguez: Untersuchungen zum Arbeitsschutz bei An- und Abfahrvorgängen von Chemieanlagen, Schriftenreihe der Bundesanstalt für Arbeitsschutz Fb 709, Dortmund 1994