Gesellschaft für
Reaktorsicherheit (GRS) mbH

German Risk Study
Nuclear Power Plants
Phase B

A Summary

GRS-74

Gesellschaft für
Reaktorsicherheit (GRS) mbH

German Risk Study
Nuclear Power Plants
Phase B

A Summary

GRS-74 (July 1990)
ISBN 3-923875-24-X

Note: The present publication is a literal translation of the report GRS-72 „Deutsche Risikostudie Kernkraftwerke, Phase B – Eine Zusammenfassende Darstellung", June 1989.

Translation: Alys Schmelzer

Keywords:
Accident management measures; core meltdown; NPP Biblis B; risk; accident; reliability analysis

CONTENT

1. Objective and Subject Matter of the Study

The German Risk Study for Nuclear Power Plants deals with investigations of accidents at nuclear power plants and the risks involved. The investigations have been carried out under a contract awarded by the Federal Minister for Research and Technology. They are subdivided into two phases (referred to as Phase A and Phase B). Results concerning Phase A have been published in 1979 [GRS 79].

The current report is a summary of the investigations carried out with respect to Phase B. An introduction into the basic ideas and objectives of the Study is followed by a survey of the main results. Both the investigations and the results are described in a comprehensive technical report [GRS 89].

Work on Phase B of the Risk Study began in 1981. Upon completion of Phase A, the Federal Minister for Research and Technolgy requested a number of institutions to continue work on the Risk Study in a subsequent Phase B. Research projects carried out for this purpose aimed above all at further deepening individual subjects of risk analyses and at preparing for use in risk investigations new findings and know-how gained by reactor safety research at both the national and the international level. The companies and institutions which participated in these research projects are compiled in Appendix A.1.

In 1985, the Federal Minister for Research and Technology requested Gesellschaft für Reaktorsicherheit (GRS) mbH to carry on and to finalize work on Phase B of the Risk Study while including the results of the individual investigations. In the scope of this project, certain sub-tasks were performed by other institutions under subcontracts awarded by GRS. The names of these institutions are also quoted in Appendix A.1.

In the course of performing the Study, reports on the respective state of investigations and progress reports on available interim results were presented at a number of meetings as well as in several publications. Appendix A.2 contains a list of the papers and publications of recent years.

1.1 Introduction

Safety issues are of crucial importance for industrial plants. Complex engineered systems are considered to be safe if besides the requirements for functional and reliable operation they also fulfill the respective safety requirements. This applies in particular to nuclear power plants and other nuclear facilities.

The supreme aim of all safety considerations is, to ensure the confinement of radioactive substances existing in a nuclear power plant. For this purpose, nuclear engineering has developed a comprehensive safety concept. Thus, from the planning stage to construction and operation, nuclear power plants have to fulfill a great number of safety requirements. Components and systems are designed with large safety margins. Multiple and recurrent tests are performed during the manufacture, the construction and the operation of plants in order to ensure a high quality standard.

For the purpose of safety assessments, comprehensive accident investigations are performed in order to determine detailed safety requirements. These investigations are carried out along the lines of important predetermined accidents, the so-called design basis accidents. They serve as a basis for the safety design of a nuclear power plant.

At an early stage in nuclear engineering, probability considerations have been made within the framework of safety assessments. As a supplement to engineering evalutations, probabilistic methods were used for a more precise quantification of the safety of a plant by computing probabilities. So, as early as in the late sixties, reliability analyses of important engineered safeguards have been performed. What was lacking then however, was adequate operating experience from which confirmed data relating to operating and failure behavior of components (pumps, valves, etc.) could be derived for the analyses. In the meantime, the situation has considerably improved as more data have become available. Similarly, the methods of reliability investigations have seen further development. Today, reliability analyses are an essential part of technical safety assessments. Finally, in the seventies, the extension of reliability analyses, and above all their application in the comparative assessment of different accident sequences, led to comprehensive probabilistic analyses or, in other words, to the first risk investigations.

Phase A of the German Risk Study [GRS 79] was the first comprehensive risk analysis ever carried out for a nuclear power plant in the Federal Republic of Germany. To a large extent the basic assumptions and methods of WASH 1400, the US Reactor Safety Study, [WAS 75] were used. Improved methods and new results of safety research were above all to be taken into account by the further work relating to Phase B.

1.2 Objectives of the Investigations

The main objective of earlier risk investigations was to assess the risk involved in accidents at nuclear power plants and, as far as possible, to compare this risk to other societal and natural risks. Thus, both WASH-1400 and Phase A of the German Risk Study mainly dealt with the assessment of injurious consequences outside the plant, and in particular with the extent and frequency of injuries to the health of the population.

However, the work carried out for Phase A of the German Risk Study also showed that risk analyses are of great benefit for technical safety assessments. The results of plant engineering investigations led to a number of safety improvements in systems by which the risk of accidents could be definitely reduced. Similar experience has been gathered in recent risk analyses particularly carried out in the United States, see e.g. [NUR 87].

The practical experience gathered with plant engineering analyses, and the improved confirmation of their results on the basis of available operating experience, have contributed to making risk analyses what they are today an efficient tool for technical safety assessments. Risk analyses and their results are used primarily to review the safety design of a plant and thus to further develop the overall safety concept of nuclear power plants.

The work relating to Phase B included comprehensive investigations of the acccident behavior. Detailed analyses have been made of the time dependence of accidents, of loads involved in these accidents, and the intervention of safety systems provided for coping with accidents.

These investigations have revealed the importance of accident management measures. Thus, analyses show that nuclear power plants in many cases still dispose of safety margins when safety systems do not intervene as scheduled and when safety design limits are exceeded. These safety margins can be used for accident management measures which serve as a tool to further reduce the risk involved in accidents. The aim of these measures is to cope with an accident even in aggravated conditions or, if this approach should fail, at least to efficiently limit the injurious consequences of an accident that cannot be coped with. The investigations carried out for this purpose within the framework of the Study show that accident management measures can be employed to create an additional safety level beyond the safety design limits.

Risk analyses are a suitable tool to identify accident management measures and to show to what extent they can be used to reduce the risks involved in accidents. Therefore, analyses of accident management measures are one of the focal points in the work performed for Phase B of the Study.

Furthermore, risk analyses deal with accidents and the possible consequences of them.

In doing so, it has become obvious that the assessment of loads arising during accidents and of the resulting consequences is affected by great uncertainties. This applies above all to extreme accidents which, although they are most unlikely, may involve a considerable release of radioactive substances into the environment of a plant.

Severe accidents are conceivable if postulating that the engineered safeguards existing in a nuclear power plant will fail to a large extent and that considerable amounts of radioactive substances contained in the reactor will be released. Irrespective of the engineered safeguards such severe accidents will involve considerable releases of radioactive substances.Accident consequences outside a plant which involve such releases have already been estimated in Phase A of the Study. Phase B does not repeat the calculations concerning offsite accident consequences.

The applications and objectives of the analyses performed under Phase B of the Risk Study can be summarized as follows:

- Comparative assessment of different accident and severe accident sequences,
- Identification of weak spots and safety improvements,
- Determination of safety margins with respect to accident and severe accident sequences exceeding the design limits,
  and, in this context,
- The assessment of accident management measures.

From an overall point of view, the fields of major emphasis and the objectives of Phase B of the Study have thus shifted to investigations concerning the plant engineering. In a more restricted sense, the risk analysis is understood as a probabilistic safety analysis which summarizes assessments of operating experience, results of accident and severe accident analyses as well as results of safety research in order to arrive at a consistent safety assessment. The task of a risk analysis is to deepen the safety assessment and to further develop the safety concept of nuclear power plants by an application of the obtained results and the insights gained.

1.3 The Reference Plant of the Study

Any risk analysis requires technical documents which describe layout, function and operating mode of a plant, its operating systems and its safety features. Detailed documents are required above all for analyses of systems engineering, e.g. detailed information on the registration of measuring values, the initiation of protective actions or the activation of safety relevant components and systems. The analyses show that individual results of the investigations often depend on design details. When carrying out a risk analysis it therefore is necessary to select a technical reference, or a reference plant, upon which the investigations will be based.

The reference plant for Phase B, which also served as a base for Phase A, is unit B of the Nuclear Power Plant Biblis. The plant is equipped with a German pressurized water reactor (manufactured by Kraftwerk Union AG) with a thermal output of 3750 MW. The plant is operated by Rheinisch-Westfälisches Elektrizitätswerk AG ("RWE") and has been commissioned in 1976.

The reasons for the continued use of Biblis B as a reference plant in Phase B include the following:

- Further work can be based directly upon existing technical documents and upon the results of Phase A.
- Although there are a number of aspects where Biblis B is no longer in compliance with the design state of more recent PWR nuclear power plants (e.g. the convoy plants), the basic safety concept such as it is found in these more recent plants has already been implemented to a large extent. For example, the layout of the protective and safety systems provides for an arrangement in separate legs.
- Of the nuclear power plants with many years of operating experience, Biblis B is the most representative one of more recent pressurized actors.
- At both Biblis A and Biblis B, assessments of operating experience have practically been made ever since these plants were commissioned.

During the investigations for Phase A already, proposals were made to modify the engineering features of systems, eliminating this way certain weak spots in the safety design of the plant. Phase A, for example, showed that human failure in coping with a loss-of-coolant accident (LOCA) resulting from a small leak made a great contribution to the overall risk. To a large extent, the measures aiming at the control of this LOCA were automated.

Similarly, improvements in systems engineering have been proposed in the form of interim results obtained from plant engineering analyses. So, modifications may considerably reduce the frequency of an uncontrolled LOCA via a leak in a steam generator heating tube. The Study considers all modifications which have already been implemented at the plant or which the licensee plans to implement in the near future. Planned modifications supported by valid documents which the licensee had presented for assessment have been assessed subject to the corresponding implementation.

1.4 Layout of the Study

Chapters 1 through 3 deal with the general prerequisites, the subject and the methods of a risk analysis.

Following Chapter 1, Chapter 2 describes the fundamentals of the safety concept developed for nuclear power plants, using the pressurized water reactor as an example.

Chapter 3 deals with the subject and the methods of the risk analysis. For this purpose, the accident and severe accident sequences to be investigated are described and the individual steps of the investigations are explained. Moreover, various kinds of reliability data and aspects for the treatment of uncertainties are addressed.

Chapters 4 through 8 contain the results of the investigations carried out. In order to provide a better overall survey, the results are not dealt with in accordance with the steps of the investigations discussed in Chapter 3, but are subsumed under general terms.

Chapter 4 deals with the analyses of plant internal accidents, of event sequences during loss-of-coolant accidents and transients, without considering accident management measures. In Section 4.3 the results of event sequence analyses are discussed and compared with the results of Phase A.

Chapter 5 contains the results of investigations of impacts which may spread to other parts of the plant. Impacts resulting from fire, flooding, earthquake and aircraft crash are discussed.

Chapter 6 deals with the investigations concerning accident management measures. Discussed in detail were those measures which may be taken to restore the cooling of the reactor core prior to a core meltdown in a postulated failure of safety systems including a depressurization of the reactor system.

Chapter 7 provides a survey of the investigations of core meltdown accidents. Various phenomena and loads are discussed which are possible in a core meltdown accident and may have an impact upon the containment.

Chapter 8 deals with the release of radioactive substances which may be involved in a core meltdown accident. The results of release calculations are discussed for various accident sequences and compared with the results of Phase A of the Study.

Chapter 9 summarizes, discusses and assesses the results of Phase B of the Study.

2. Fundamentals of the Safety Concept Illustrated by the Example of a Pressurized Water Reactor

2.1 The Pressurized Water Reactor

Fig. 2-1 shows the basic layout and functions of a PWR nuclear power plant.

The heat generated by nuclear fission in the reactor core (1) is transferred by the closed reactor coolant circuit (primary circuit or pressure boundary of the reactor coolant) through the steam generator (2) to the feedwater/steam circuit (secondary circuit). A sufficiently high pressure of the coolant prevents the formation of steam in the reactor cooling circuit, hence the origin of the term "pressurized water reactor". The water supplied to the steam generators on the secondary side evaporates as a result of the uptake of heat coming from the reactor coolant circuit. The steam operates the turbine (5) which, in turn, operates the generator (6). The steam escaping from the turbine cannot be used any longer for the generation of power and is condensed in the condenser (7). The condensed water is pumped back to the steam generators. Heat removal from the condenser occurs via the main cooling water system. Depending on the prevailing environmental conditions, this heat is discharged to the environment either in a direct approach to a river or via cooling towers. At nuclear power plants, the transformation of heat into electric power is performed in the same way as it is done at other thermal power plants.

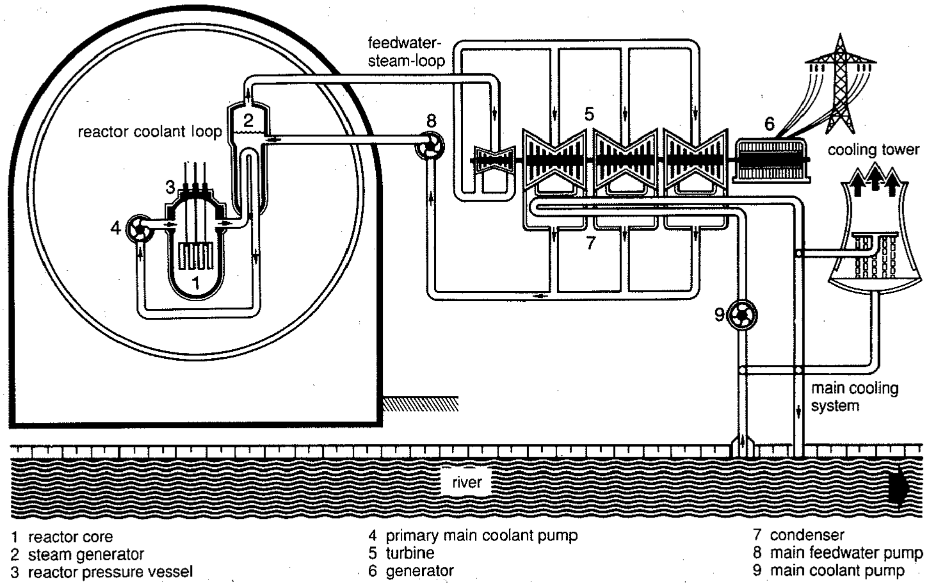


Fig. 2-1:
Functional diagram of a PWR nuclear power plant

2.2 Basic Safety Requirements

Nuclear power plants have to comply with special safety requirements, as considerable amounts of radioactive substances are generated by nuclear fission during reactor operation. For example, the activity inventory of a large 1300 MW(e) power reactor is about 1020 Bq[1]. Even if only a small part of this activity inventory should escape from the plant into the environment, hazards to health and life would result. Thus, the primary task of reactor safety is the safe confinement of the activity inventory.

The reactor continues to generate heat even after having been shut down. This is referred to as decay heat. It is generated by the radioactive decay of the fission products formed during operation of the reactor. Immediately after a reactor shutdown, the decay heat amounts to about 6%, after approximately six hours to about 1%, and after one day to about 0.7% of the rated power of the reactor. Without cooling of the

[1]) The unit of activity is the Becquerel (Bq). 1 Bq corresponds to one radioactive decay per second. The former unit 1 Curie (Ci) corresponds to 37 billion decays per second.

reactor core, the decay heat would be sufficient to heat up the reactor core to such an extent that the fuel would melt and radioactive fission products would be released. Therefore, the reactor core requires to be cooled even after the shutdown of the reactor.

For reactor operation, the following basic safety requirements result:

- Confinement of radioactive substances: Radioactive substances must be retained in the reactor core.
- Control of reactivity: The reactor must be capable of being shut down safely at any time and being maintained in the shutdown state.
- Core cooling: Even after a reactor shutdown, reactor core cooling and residual heat removal must be assured on a long-term basis.

2.3 The Safety Concept

The pressurized water reactor is used as an example to illustrate the main characteristics of the safety concept.

The safety concept consists, for one thing, of the multiple confinement of radioactive substances contained in a reactor and, for another thing, of engineered safeguards and measures which assure the confinement of the radioactive substances.

• Activity Barriers

The major part of the radioactive substances (approximately 95%) is generated by nuclear fission of the nuclear fuel during reactor operation. These fission products are confined by a series of echeloned structures, the so-called activity barriers. These are (see Fig. 2-2):

- The crystal lattice of the fuel itself,
- The fuel rod cladding tubes with their gas-tight welds,
- The reactor pressure vessel together with the closed reactor coolant circuit,
- The gas-tight and pressure-resistant containment which confines the reactor coolant circuit, and
- The outer reinforced concrete shield. Its tightness function is only limited. It permits the extraction of leakages from the containment and protects the plant against external impacts.

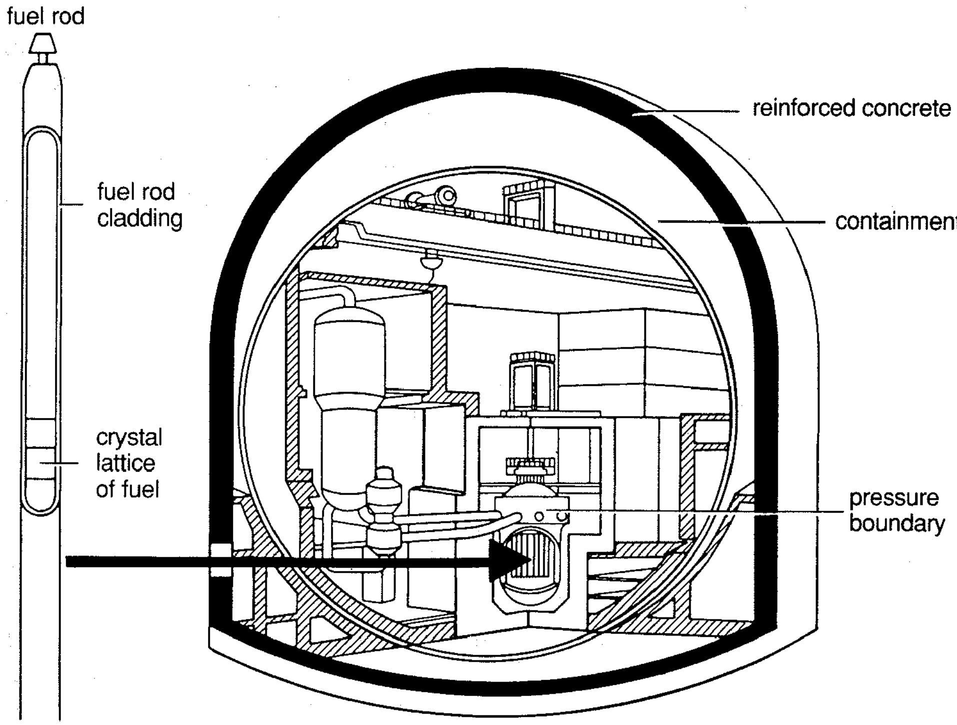


Fig. 2-2:
Activity barriers, confinement of the fission products

• Safety Design

In order to limit the influence of malfunctions or the consequences of accidents and to assure the confinement of radioactive substances, nuclear power plants are provided with multi-stage safety measures attributed to different safety levels.

First Safety Level: Quality Assurance Measures

This safety level comprises requirements to be met by the design standards and by the quality above all of the nuclear parts of the plant. Components and systems are designed with large safety margins. Moreover, this level comprises quality assurance measures to be taken during the manufacturing process of components and the construction of the plant. The high quality standard is assured by careful management of operation and by its documentation as well as by in-service inspections during the whole operating life of the plant.

Second Safety Level: Measures for the Prevention of Accidents

In order to prevent accidents which may develop from malfunctions, a nuclear power plant is equipped with control and protection systems. Task of these systems is to detect in time any malfunction and to initiate actions for an immediate limitation of malfunctions already occurred.

The most important protective system is the reactor protection system. It is concerned with the continuous monitoring of all essential data to be measured in the plant, such as reactor power, pressure in the reactor cooling circuit, rotational speed of the reactor coolant pumps, etc.

The first two safety levels serve to avoid malfunctions as far as possible and/or to prevent any malfunction from expanding into an accident.

Third Safety Level: Measures for the Limitation of Accidents

In spite of all precautions taken to assure safe operation, the occurrence of an accident cannot be ruled out. Therefore, at a third level of safety measures, nuclear power plants are provided with comprehensive engineered safeguards, the safety systems. Activated by the reactor protection system, the safety systems intervene automatically to a large extent when occurring an accident in order to maintain the confinement of fission products and to limit the damaging consequences resulting from such an accident. The safety systems are designed so as to cope with a broad spectrum of different accidents.

- **Sequences beyond the Design Basis**

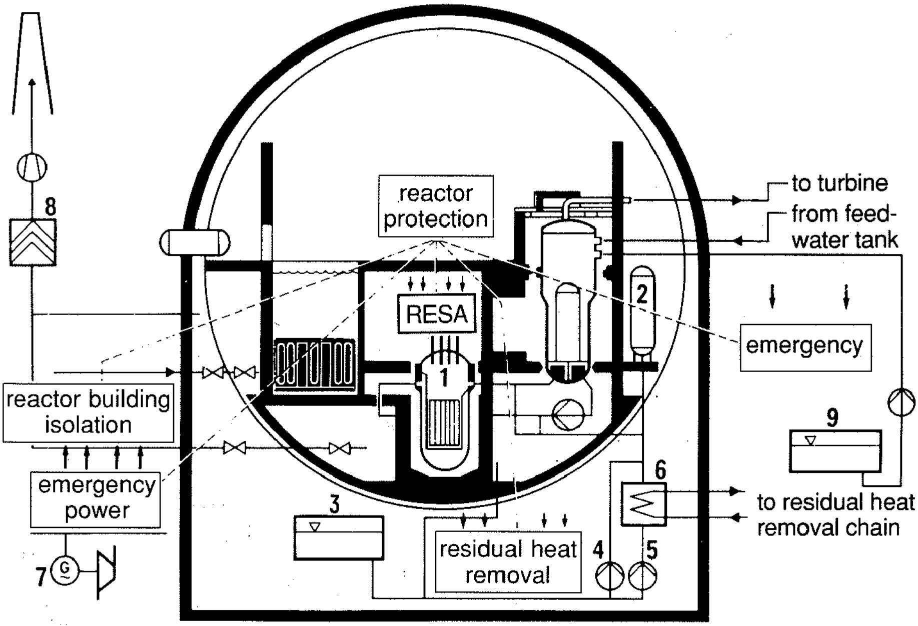
Even if postulated a failure of safety systems during an accident, in many cases it is still possible to cope with this accident and to bring the plant into a safe state. Nuclear power plants still dispose of safety margins even if the design limits are exceeded.

In Phase B of the Risk Study accident analyses have been carried out which served to investigate the possibilities of accident management measures. By means of these analyses planning bases for accident management measures have been created. Investigations reveal that for accident sequences beyond the design basis an additional safety level can be created by accident management measures.

2.4 Engineered Safeguards of the Pressurized Water Reactor

Figs. 2-3 and 2-4 provide a survey of important systems and engineered safeguards in a pressurized water reactor. They are briefly described as follows:

- In the core, the energy released during the nuclear chain reaction is transformed into thermal energy. The core contains most of the plant's radioactive substances.
- The reactor scram system serves for the fast interruption of the chain reaction. In such a case, the energy release in the reactor core will be reduced to the energy release resulting from fission product decay (residual heat).
- The reactor coolant circuit consists of the reactor pressure vessel, the reactor coolant pipes, the primary side of the steam generators with the steam generator heating tubes as well as the inlet and outlet headers, the reactor coolant pumps and the pressurizer. In the reactor coolant circuit, the heat will be transferred to the coolant in the reactor core and then be transported to the steam generators.
- The feedwater/steam circuit consists of the secondary side of the steam generators, the main steam pipes with the main steam bypass system, the turbine with the turbine condenser and the main condensate pumps, the feedwater tank and the main feedwater system with the main feedwater pumps. During power operation, the feedwater/steam circuit transfers the heat from the steam generators to the turbine.
- The volume control system compensates fluctuations in the coolant volume during reactor operation.
- The automatic control serves to keep the essential process variables within preset ranges of operation in the case of different power requirements and malfunctions.
- The reactor protection system records all safety-relevant measuring data and, as soon as certain limits are reached, activates reactor protection signals which automatically initiate protective actions.
- The electric power supply consists of the auxiliary power system and the emergency power system. The auxiliary power system supplies power to the components and systems which are important for the operation and the safety of the plant. Should this power supply system fail (loss of preferred power), the emergency power system will supply power to the safety-relevant components.



1 scram system
2 accumulator
3 borated reactor water storage tank
4 HP safety injection pump
5 residual heat removal pump
6 residual heat exchanger
7 emergency power system
8 venting systems
9 emergency feed system

RESA = reactor scram

Fig. 2-3:
Engineered Safeguards of the pressurized water reactor

- The emergency feedwater system supplies the steam generators whenever the main feedwater system is not available. The emergency feedwater system can be used for the removal of residual heat and for the shutdown of the plant (i.e. for decreasing the coolant temperature).
- The emergency core cooling and residual heat removal system comprises the following system functions: high-pressure injections, accumulator injections and low-pressure injections. Its task is the long-term removal of the residual heat via the component cooling system and the nuclear service water circuit. In addition, it has to inject coolant into the reactor coolant circuit shoud a LOCA occur.
- In the case of external impacts the emergency system has to bring the plant into a safe state. For this purpose, a load circuit which is important for the safety of Biblis B, is supplied from the protected area of the adjacent Unit A. For example, by isolating certain lines

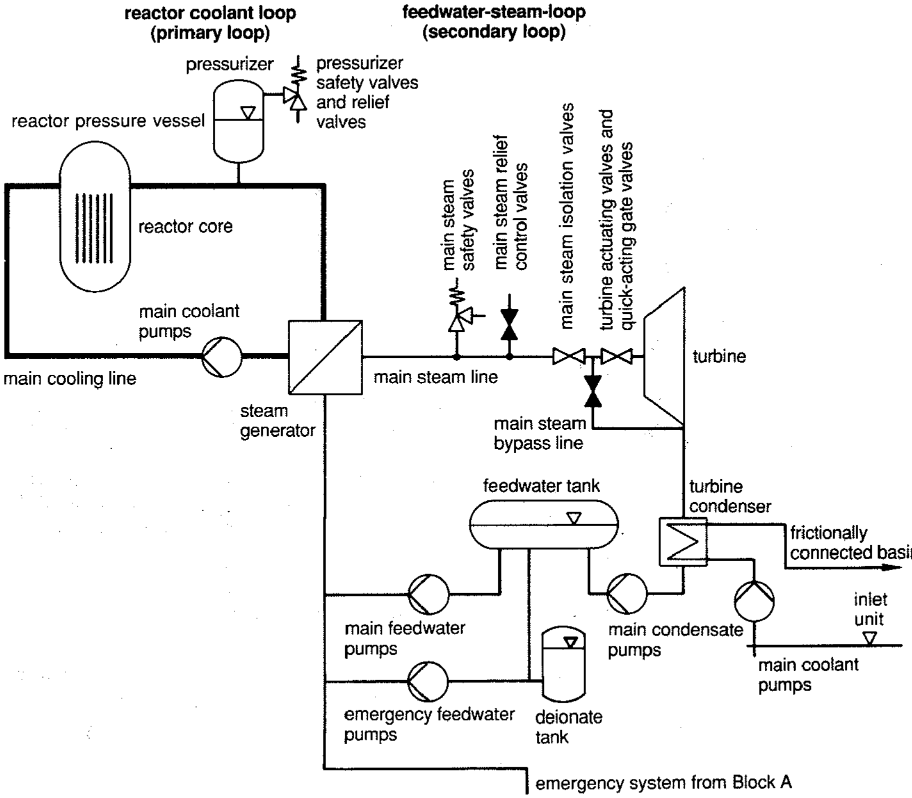


Fig. 2-4:
Diagram of the reactor coolant and feedwater/steam circuits

from Unit A, two of the four steam generators at Unit B can be supplied with emergency feedwater.

- The containment with its reactor building isolation system (isolating valves) encloses the most important activity containing components of the plant. The surrounding reinforced concrete shell protects the containment against external impacts. The space between the outer reinforced concrete shell and the containment is referred to as annulus.

3. Subject and Methods of the Risk Analysis

3.1 Risk Analyses Why?

With the safety concept as developed for nuclear power plants, far-reaching and comprehensive precautions were taken against accidents and the resulting release of radioactive substances. Operating experience in the Federal Republic of Germany has shown that the occurred malfunctions and accidents could be coped with by the existing engineered safeguards. At a worldwide level, the operating experience available covers a period of about 30 years and more than 2,500 reactor operating years. During this time, in nuclear power plants of Western design no accident has occurred which led to a considerable release of radioactive substances into the environment.

In March 1979, a core meltdown accident occurred at the US nuclear power plant of Three Mile Island ("TMI"). In the course of this accident, the reactor was heated up to such an extent that fuel rod claddings burst and major parts of the reactor core melted down. However, apart from some minor releases of activity via the reactor building drainage system, all of the radioactive substances released from the nuclear fuel could be kept inside the plant.

The reactor accident at Chernobyl in April 1986 has so far been the most serious accident that ever occurred at a nuclear power plant. In the course of this accident, a nuclear power excursion in the reactor led to the destruction of the reactor core within a few seconds. Due to their physical characteristics and the additional safety precautions, such a reactivity accident cannot occur at light water reactors of Western design.

In risk analyses of nuclear power plants the conditions have to be investigated under which radioactive substances confined in the plant may be released into the environment and lead to injuries outside the plant. Should accidents occur which are coped with by the safety systems in compliance with the design of the plant, no injurious effects will arise outside the plant, as the confinement of the radioactive substances is maintained at all times. Therefore, risk contributions can only be expected from event sequences for which it is postulated that safety systems will fail to a large extent and that accident management measures will not be successful or effective respectively. Only in such cases a dangerous release of radioactive substances into the environment of the plant will be possible.

Risk analyses therefore deal with event sequences in the course of which safety systems fail and design limits are exceeded. Based on the state of the safety design, accident and severe accident sequences are investigated with respect to both occurrence frequencies and potential injurious effects.

Thus, risk analyses by far exceed the tasks of the "classical" safety analysis such as it is required for the demonstration of safety in the course of the nuclear licensing procedure. The safety analysis does not deal with accident sequences for which a failure of safety systems is postulated and for which design limits of the plant are exceeded. Moreover, the analysis does not give any information on the occurrence frequency of accidents and the failure probability of engineered safeguards. Thus, it does not include any details concerning the frequency of accidents which may lead to a dangerous release of activity into the environment.

It is not possible however, to simply replace the "classical" safety analysis by a risk analysis. The main task of the safety analysis is to specify and to determine the safety design of a plant. For this purpose, certain predetermined accidents are investigated in detail with respect to their potential sequences and consequences. These so-called design basis accidents (DBA) are selected in such a way that the accident analyses required for them also cover the sequences and effects of other accidents. Because of the boundary conditions this way specified (determined) for the investigations of accidents, the "classical" safety analysis is also referred to as a deterministic safety analysis, contrary to the probabilistic risk analysis.

With its specification of the safety design, the deterministic analysis is a necessary precondition for risk investigations. Risk analyses should be considered a supplement to the deterministic safety assessment. With their probabilistic methods, they can be used to review the safety design of a plant and to further develop the existing safety concept. In this context, the benefit of the probabilistic analysis, as compared with the deterministic assessment, is the fact that the importance of accidents and severe accidents can be assessed in a quantitative approach on the basis of the expected frequencies. Thus, weak spots in the safety design, as compared with other contributions from accident sequences, can be identified on the basis of relatively high frequencies of accident consequences which cannot be coped with. If such weak spots are eliminated, a well-balanced safety design will be reached.

3.2 Accident and Severe Accident Sequences to be Investigated

About 95% of the entire activity inventory of a nuclear power plant is contained in the reactor core. Thus, the Study mainly deals with accidents which affect the reactor core. About 98% of the activity inventory in the reactor core are bound in the crystal lattice of the nuclear fuel. Greater amounts of radioactive substances can only be released if the fuel is considerably heated up and melts.

A core meltdown is only possible if the reactor core is not cooled over a prolonged period of time and the heat cannot be removed from the reactor core. Thus, risk analyses have to investigate the degree of probability at which, and the conditions under which accidents may lead to a core meltdown in spite of the existing safety features.

Accident analyses, however, show that accident sequences for which a failure of safety systems is postulated, do not lead to an immediate core meltdown. In many cases, such sequences initially involve only slow changes of the state of the reactor coolant circuit. In general, a longer period of time passes before the plant reaches a state in which the reactor core may be damaged. In most cases, this period of time is at least one hour. It can be utilized to take accident management measures to cope with the accident, or to restore the cooling of the reactor core, before the fuel begins to melt.

This will be briefly illustrated by an example. When occurring a loss of preferred power, the main feedwater pumps in the feedwater/steam circuit are automatically turned off. If, in addition, a total failure of the emergency feedwater supply is postulated (failure of the emergency feedwater system and the emergency system), then the secondary side feeding of the steam generators fails completely. In such a case, the heat generated in the reactor cannot be removed any longer via the steam generators. The reactor coolant circuit heats up. The relief valves of the pressurizer respond. However, a dangerous heating-up of the fuel rods only begins when the reactor coolant circuit has steamed out via the relief valves to such an extent that the water level in the reactor pressure vessel falls below the top edge of the core and the fuel rods in this core area are uncovered. In the case described here, i.e. the complete failure of the steam generator feeding following a loss of preferred power, approximately two hours are available to restore the reactor core cooling by flexible emergency measures before the water level in the reactor pressure vessel can fall below the top edge of the core.

The processes involved in a core meltdown itself and the related phenomena are of a complex nature. They are briefly described below.

If the reactor core is not cooled the decay heat generated in the fuel heats up the reactor core and causes an evaporization of the water in the reactor pressure vessel. The fuel rods this way uncovered from coolant are heated up to such an extent that the fuel melts.

During the fuel melting process, the core support structures fail as well. Molten core and structural materials crash into the residual water still available in the bottom head of the reactor pressure vessel. The water evaporates. Finally, the reactor pressure vessel melts through in the area of the bottom head. Molten core and structural materials slump into the reactor cavity and penetrate the concrete of the building foundation.

If the integrity of the containment vessel is maintained over a longer period of time, most of the fission products released from the molten materials are deposited on the internals and walls of the containment or are retained in the water of the building sump. Thus, accident sequences in which the containment vessel remains tight for a longer period of time, e.g. for several days, only involve a rather limited release of activity.

On the other hand, accident sequences are possible which may lead to an early release of activity. The release as a rule, will then be considerable. These are accident sequences in which

- the containment is not tight right from the beginning,
- the retention function of the containment is bypassed, or
- loads occur which lead to an early failure of the containment.

The Study includes a more detailed investigation of various phenomena and processes which may occur in the course of a core meltdown accident.

3.3 Individual Steps of the Analyses

Fig. 3-1 provides a survey of the steps of the analyses.

• Recording of the Triggering Events

Malfunctions of and damage to components and plant items which cause an activation of safety systems are referred to as "triggering events". Such triggering events include, among other things, a leak in a coolant pipe of the reactor coolant circuit or a failure of the feedwater supply to the steam generators in the feedwater/steam circuit.

The first step is to identify all important triggering events which may damage the reactor core and to determine their frequencies.

It is neither possible nor necessary to specify and to analyze in detail all triggering events which are conceivable. It is important however, to

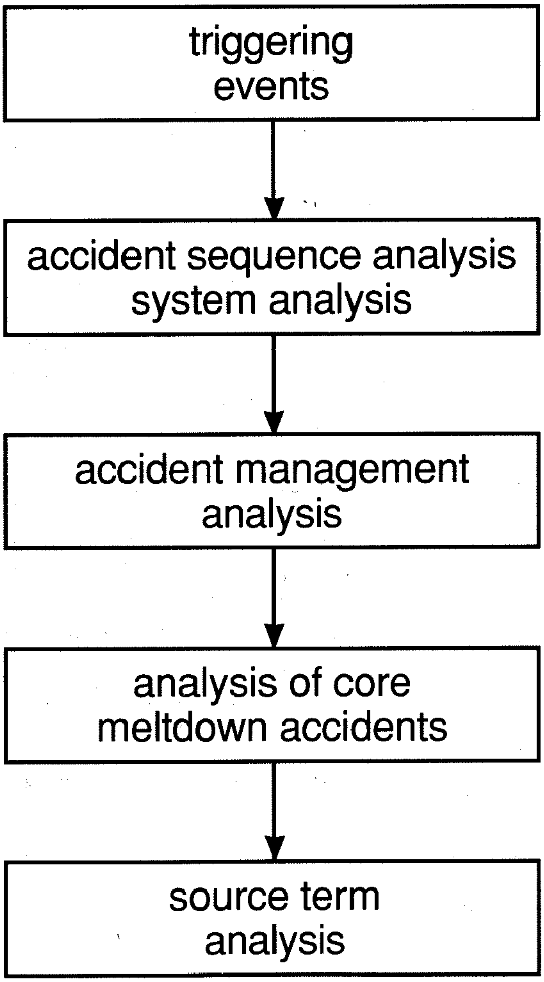


Fig. 3-1:
Steps in analysis

choose a limited number of triggering events which are representative of a group of similar individual events and which lead to similar accident sequences.

● Event Sequence and System Analyses

Detailed investigations are performed with regard to the selected triggering events. These investigations consist of two parts, i.e. the event sequence analysis and the system reliability analysis.

The event sequence analysis starts out from a triggering event (e.g. the rupture of a pipe) and identifies the various possible effects of this event on the basis of success or failure of the safety-oriented countermeasures (system functions) to be taken. Depending on the extent of

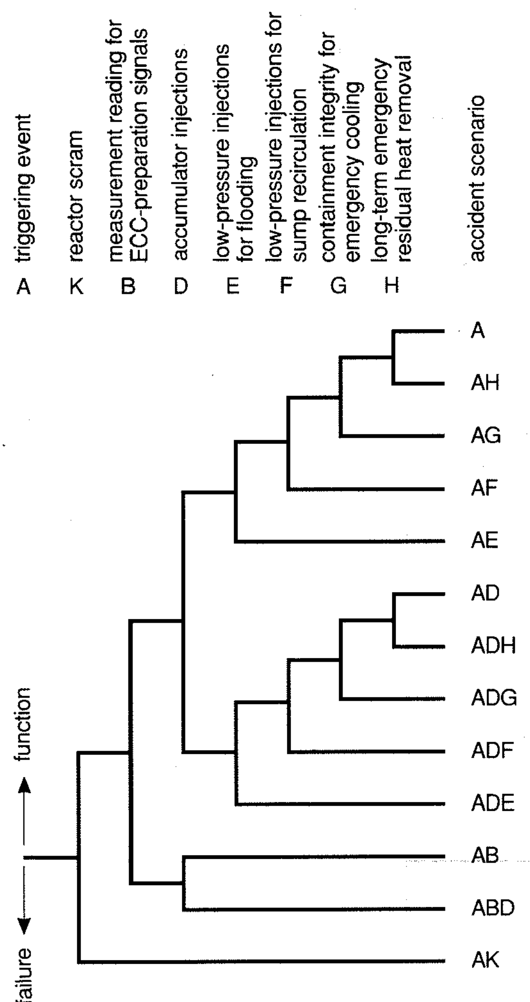


Fig.3-2:
Event sequence diagram "large leak in a reactor coolant pipe"

The safety functions required in the course of an accident (safety systems) are plotted in the sequences event tree more or less in compliance with the chronological order of their requirements. Each ramification corresponds to a required safety function (reactor scram, preparatory emergency cooling signal, etc.). An upward ramification means that the required function is operable, a downward ramification means that it fails. Thus, an event sequence consisting entirely of upward ramifications means that the accident is completely coped with.

If the activation fails (failure of the measured value detection), the emergency coolant from the accumulators will be injected automatically as the pressure in the reactor coolant circuit decreases.

the required countermeasures, a varying number of event sequences will result which are depicted in an event sequence diagram (sequence event tree).

Fig. 3-2 shows as an example a simplified event tree of the triggering event referred to as "large leak in a reactor coolant pipe". The triggering event leads to a reactor scram automatically activated by the reactor protection system. Depending on the success or failure of this measure, two different event sequences result. In the further course of the event, the various systems provided for emergency cooling and for the residual heat removal are activated automatically, depending on whether or not the emergency cooling systems are activated (measured value detection for preparatory emergency cooling signals available or not).

Depending on the success or failure of the required safety systems, the individual event sequences lead to different states of the plant. In Fig. 3-2, event sequence A shows that all the required safety systems function as scheduled. It therefore corresponds to a state of the plant in which the accident concerned is completely coped with. Event sequence AH however, in which the long-term residual heat removal (H) has failed, corresponds to an event sequence which is not coped with by the safety systems. Event sequences not coped with by the safety systems lead to plant damage states. The Study centralizes under one and the same fault condition those event sequences which lead to identical or similar injurious effects.

In order to determine the frequency of the individual event sequences, data on failure probabilities of the required safety systems and on occurrence probabilities of the triggering event must be available. These failure probabilities, however, cannot be calculated before knowing the effectiveness conditions to be fulfilled by the safety systems in order to cope with an accident. Indications concerning the failure probability of the long-term emergency residual heat removal system (H) cannot be made before determining whether or not the long-term residual heat removal may be performed by only one or by two of the four existing subsystems (system legs) of the emergency and the residual heat removal system. To determine these minimum requirements for the effectiveness of the safety systems, calculations of plant dynamics are needed for a more precise analysis of accident sequences and the loads involved.

If the minimum requirements are known the failure probabilities of the required safety systems can be calculated. The reliability analyses of the safety systems which are necessary for this purpose are mostly carried out by means of the fault tree method.

In a fault tree analysis, a so-called "undesired event", for example the failure of a system (such as the failure of the emergency and residual heat removal system), is investigated for all possible reasons which may lead to this event. The method is a deductive one. Starting out from the postulated failure of the system under review, logic connections (AND, OR, NOT) are used to develop and to detect all possible failure combinations of subsystems down to the level of elementary failure events, i.e. the level of component failures (failures of pumps, valves, switches, etc.). Once the fault tree analysis has been performed, the subsequent reliability calculation uses reliability data concerning the failure behavior of the components for an extrapolation of the failure probability of the system being analysed. For this purpose, complex systems leading to large fault trees generally require the use of reliability computer codes.

Once the failure probabilities of the safety systems have been calculated, the ramifications in the event sequence diagram (Fig. 3-2) can be used for a probability assessment. The frequency[1]) of the event sequences which are not coped with by the safety systems (damage states) is obtained by multiplying the occurrence probabilities of the triggering events by the respective failure probabilities of the safety systems and then summing up all the frequency contributions made by event sequences which are not coped with.

● Analyses of Accident Management Measures

Phase B of the Study investigates to what extent measures can still be taken to prevent a core meltdown or to mitigate the consequences of such an event once a failure of safety systems has occurred.

Of particular importance are those accident management measures which are still capable of preventing a core meltdown. There are a number of possibilities for this purpose. The Study includes a detailed investigation of measures to restore the core cooling and to remove the heat from the reactor after a depressurization of the reactor coolant circuit (primary bleed) and before fuel melting can set in. These measures can be initiated both on the secondary side in the feedwater/steam circuit and on the primary side in the reactor coolant circuit.

● Analyses of Core Meltdown Accidents

As far as the core meltdown accident is concerned, three major groups of subjects are discussed:

- Processes during melting as such, the behavior of the molten core and the transient loads of components of the reactor coolant circuit;
- The loads acting on the containment and its possible failure modes;

---

[1]) To be more precise, what is concerned here is an "expected" frequency, a calculated non-integer frequency value. For the sake of simplicity, the term frequency is used here and in the further course of the Study.

- Behavior of radioactive substances released during a core meltdown and, when failing the containment vessel, their release into the environment.

These analyses furnish source terms for various accident sequences.

3.4 Reliability Data

• Kind of the Data

Risk analyses require various data. Besides the technical design data describing the plant, mainly two groups of data are needed:

- Data for the simulation of accident and severe accident sequences,
- Reliability data for the performance of event sequence and reliability analyses.

To a large extent, technical design data and data for the simulation of accident and severe accident sequences may be taken over from earlier investigations.

Reliability data are data relating to the operating and failure behavior of a plant as well as its individual parts and components. As a rule, they are not available from other investigations. Required are the following data:

- Frequency of the triggering events,
- Characteristic reliability data of components, i.e. failure rates and/or failure probabilities, including details relating to inspections, maintenance and repair,
- Reliability data relating to actions of the operating personnel.

• Data Sources

As far as possible, reliability data are deduced from operating experience. Three sources of data have to be distinguished:

- The plant to be investigated,
- Other nuclear power plants,
- Other power plants and factories (e.g. coal-fired power plants or chemical plants).

Data originating from the plant to be investigated are referred to as plant-specific data, data from other plants as generic data.

As far as possible, the Study is based on plant-specific data. Plant-specific data may furnish, for example, details on the operating times of components, on the exchange of component parts and on engineering improvements that have been carried out. Generic data are only used if the plant-specific operating experience is insufficient.

Plant-specific data are used for triggering events which have occurred at a certain frequency during the operating life of the plant, as well as for the failure behavior of most of the components. At the plant under review, these data have been gathered over several years. Wherever plant-specific operating experience is not sufficient, use is made of German and worldwide operating experience at nuclear power plants.

If a certain triggering event has never been observed in the course of the operating experience, the estimate of the frequency of this event is exclusively determined by the period of observation. Are such periods comparatively short, the occurrence frequency of the triggering event may be considerably overestimated. In order to arrive at more realistic estimates in such cases, theoretical considerations have to be taken into account as well. So the occurrence frequencies of medium-sized and large leaks in pipes can only be derived theoretically from probabilistic fracture mechanic analyses.

• Common Cause Failures

Redundant systems are characterized by very high reliabilities, since a simultaneous failure of several redundancies must occur in order to make the system unoperable. At highly redundant systems it is thus most unlikely that a system failure will be caused by an accidental coincidence of several independent faults in different redundancies.

This applies e.g. to a four-leg system in which already one of the four existing subsystems is sufficient to perform the function of the system. A failure of the system only occurs if all the four subsystems fail or have failed at the same time.

With an increasing degree of redundancy, however, those faults become more important which may lead to a simultaneous failure of several redundancies or subsystems. Such faults may be consequential failures (e.g. damage to components in the case of a pipe rupture) or functional failures originating from a common cause. Failures which affect more than one component or system at the same time are referred to as common cause failures.

Common cause failures may be traced back to various causes. They may stem from planning or manufacturing faults, but may also be due to unfavorable environmental or operating conditions (humidity, inadmissible loads, etc.). The failure of an oil supply system common to several redundant pumps, or the failure of batteries due to aging or insufficient maintenance would be termed a common cause failures.

At nuclear power plants, comprehensive measures are taken against common cause failures. So, the individual legs of safety systems are physically separated as far as possible, and links between the redundant subsystems (legs) are avoided to a large extent. The avoidance of interconnected subsystems means that failures of individual components cannot affect several legs at the same time. Another measure taken against common cause failures consists in applying the principle of diversity, i.e. different principles of functioning and design are used for redundant engineered safeguards.

Only a few observations have been made with respect to common cause failures. Most of them stem from national and international operating experience gathered at other nuclear power plants, and only in a few isolated cases from Biblis B. Events occurred at plants and identified as common cause failures are normally remedied by modifications, so that repetitions are practically impossible. The operating experience at nuclear power plants furnishes data in particular for such failures which have occurred during operation or have been detected during functional tests. These data cannot always be applied to requirements under accident conditions. For this reason, common cause failures only occurring or only detectable during an accident, can, to a large extent, only be assessed analytically.

For the assessment of common cause failures, the Study used evaluations of national and international operating experience covering more than 1,000 operating years of nuclear power plants. In this context, it had to be examined in each individual case to what extent the experience from events occurred at other nuclear power plants could be transferred to Biblis B.

On the basis of the evaluated operating experience, the Study determined probabilities of common cause failures of essential components (emergency diesels, pumps, control equipment, etc.). For this purpose, various mathematical models were used which can also serve to describe the failure probability of interconnections between redundant components and/or subsystems.

• Human Actions

Operating experience and the results of risk analyses show that human actions, such as interventions by the operating personnel, can have a considerable effect upon the safety of a plant. They may have both a positive and a negative impact on the plant.

Scheduled interventions of the operating personnel are taken into consideration in event sequence and fault tree analyses. As far as unscheduled interventions are concerned, the analyses can be reviewed as to whether these interventions may lead to event sequences which have not yet been covered by the analyses.

With respect to the qualitative and quantitative evaluation of human actions, improved methods have been developed and data documentations have been prepared in recent years, in particular in the United States; see e.g. /SWA 83/. As far as possible, they have been used in the work contributing to this Study. Nevertheless, the evaluation of human reliability remains difficult. As before, in many cases only simple estimates are possible hereto.

On the other hand, contributions resulting from human failure are already included to a large extent in the reliability data of components and systems. So, operator errors during operation or interventions which may lead to malfunctions are already covered by the occurrence probabilities determined for triggering events on the basis of operating experience. Similarly, the failure rates of components include contributions originating from faulty maintenance.

3.5 Uncertainties of the Analysis

Risk analyses use for an overall assessment information and knowledge derived from various fields and individual investigations. Hereto belong among other things:

- Information derived from operating experience, e.g. data concerning failures of components and malfunctions that have occurred,
- Results of accident analyses, and
- Results of research projects, e.g. for the assessment of core meltdown sequences including the phenomena and thermodynamic loads involved.

All this information used in risk analyses is subject to uncertainties. On the one hand, these uncertainties result from simplified descriptions of complex relationships, e.g. the description of individual phenomena, but on the other hand, they are also a result of fundamental limitations. In principle, three different classes of uncertainties can be distinguished in this respect:

- Uncertainties of data (e.g. of reliability data) and characteristics (e.g. parameters in accident analyses) which result from incomplete data sources and/or inssufficient information,
- Uncertainties in modeling resulting from simplified assumptions which are only an approximate description of real conditions, and
- Uncertainties with respect to the completeness of the analyses because a complete recording of all important events and sequences cannot be demonstrated.

The analyses carried out for Phase B show large uncertainties in the treatment of various subtasks. This applies, for example, to the assessment of very unlikely and extreme accident scenarios, uncertainties of which to describe phenomena and to determine the occurrence frequencies of the corresponding accident sequences, cannot be quantified at present with a sufficient degree of precision and verification capability.

In phase B the uncertainties of plant dynamic analyses performed for accident simulation purposes have not been systematically reviewed. Similarly, no uncertainties have been quantified for the modeling of accident sequences. In view of the existing uncertainties and gaps in our knowledge, assumptions and assessments are applied which in many cases are more unfavorable than in reality. The here existing difficulties, however, are partly eased by the fact that, in many cases, a detailed and realistic description of accident and/or severe accident sequences is not necessary. What is more important is the determination of the very moment at which certain effects may occur, such as the beginning of core meltdown or the formation of hydrogen. Similarly, various phenomena and processes which influence the behavior of the fission products released from the molten mass can often be described by simple models.

A systematic treatment and quantification of the uncertainties involved in a risk analysis requires further (in parts rather sophisticated) investigations. Corresponding work has been initiated. So investigations presently under way deal with the confidence levels of computer codes used for the simulation of acccidents.

Uncertainties in systems engineering analyses as well as in reliability and event sequence analyses have been treated in Phase B. In these fields, the methods how to quantify uncertainties have been developed farthest. By means of these methods uncertainties in the input data of the fault tree and of the event sequence analyses, as well as statistical uncertainties in the reliability data for component failures and for frequencies of triggering events may be estimated and also be followed up in the calculations. A brief explanation of these uncertainties is given as follows.

To gather operating experience, triggering events and failures of components are observed. Reliability data determined on the basis of these observations are affected by uncertainties for the following reasons:

- It is always only a limited number of observations that are made with respect to component failures and malfunctions. The evaluation of a limited number of observations, e.g. concerning pump failures, furnishes an estimate, e.g. for the failure rate of pumps, which is affected by uncertainties.
- As a rule, the observations do not refer to the failure of components of identical design under comparable operating conditions. Failures of pumps, for example, are recorded, design of which is different from each other. Therefore, additional uncertainties result from the design, and the operating conditions of components.
- If only a very small number of observations, or none at all, are available concerning the occurrence of a triggering event or the failure of a component, engineering estimates or the results of theoretical analyses have to be applied. These assessments are also affected by uncertainties.

The uncertainties of the reliability data are described by probability distributions. In principle, various kinds of distribution functions can be applied for these probability distributions. In general, the lognormal distribution is used to describe the probability distributions of reliability data. Fig. 3-2 shows the probability density function for the lognormal distribution.

The log-normal distribution is defined by two parameters. As a rule, it can easily be adapted to empirical distributions of existing estimates.

In general, the following data are quoted for a distribution:

- Its median value, the 50% fractile of the distribution[1])
- The 5% and 95% fractiles as a measure of the distribution width and, in addition,
- Its expected value.

[1]) The p% fractile of a distribution denominates the value below which the applicable value of the quantity described by the distribution is found at a p percent probability (subjectivistic interpretation).

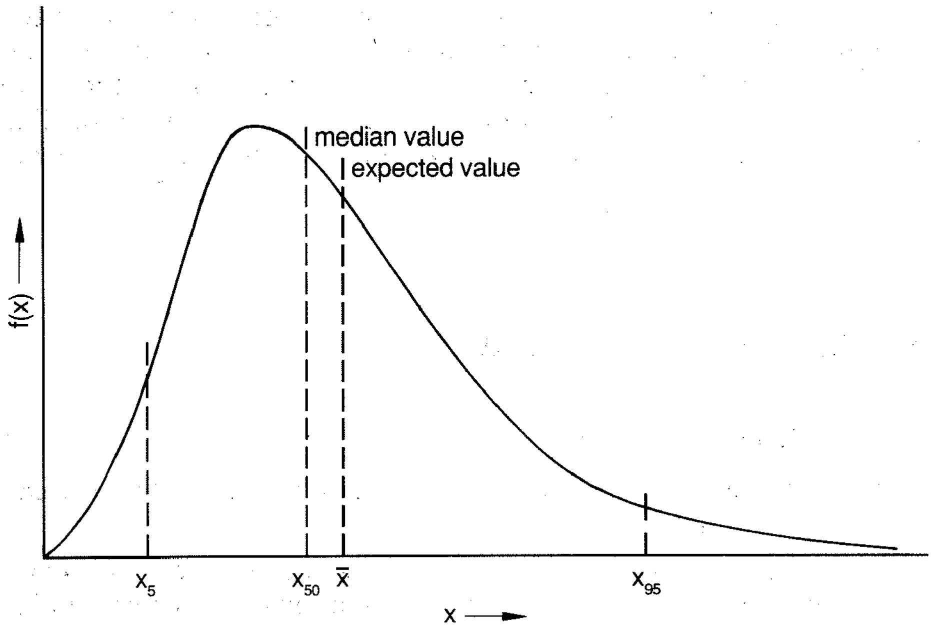


Fig. 3-3:
Function of probability density for log-normal distribution (p% fractile x_p, expected value p)

The expected value is understood as the value of the random variable being described by the distribution and to be expected as the mean over many observations. In a log-normal distribution, the expected value is always greater than its median value. This means that in a log-normal distribution more emphasis is placed on areas of high values than, for example, in a plain normal distribution.

In compliance with the rules of probability analyses, quantified uncertainties of estimates in failure rates, probabilities and expected frequencies of triggering events are followed up in reliability analyses of systems engineering and in event sequence analyses, and their results are taken into account. In doing so, corresponding probability distributions are again obtained for the results of these analyses.

The propagation of the uncertainties in the further analyses of accident management measures and in the analyses of core meltdown accidents has not been followed up, since, with respect to these parts of the investigations, the influence and the uncertainties of important parameters cannot be sufficiently quantified at present.

In the following chapters which deal with the results of the Study, only point values are indicated for the frequencies of event sequences which are not coped with (frequencies of damage conditions). They have been determined by using the expected values of triggering event frequencies and of the reliability data for the components. At all analyses that have been performed, these point values are located between the median values and the expected values of the appurtenant probability distributions.

4. Plant Internal Accidents

4.1 Triggering Events

Plant internal events which may cause damage to the reactor core can be subdivided into two groups:

- Loss-of-coolant accidents: accidents which lead to a loss of coolant through a leak in the reactor coolant circuit or in a connecting pipe and
- Transient accidents: accidents during which the heat generation in the reactor core is increased or the heat removal from the reactor core is affected.

Concerning the events which may trigger a loss-of-coolant accident, the Study investigates accident sequences originating from

- leaks in a reactor coolant pipe,
- leaks in the pressurizer,
- leaks in a connecting pipe of the reactor coolant circuit outside the containment and
- leaks in steam generator heating tubes.

The term "leak in a rector coolant pipe" includes all leaks in the reactor coolant pipe itself, in connecting pipes before the isolating valves, and leakages in the reactor coolant pumps.

A pressurizer leak occurs if a relief valve at the pressurizer (either a blowdown or a safety valve) opens and remains open by mistake. A leak in the equalizing pipe connecting the pressurizer to one of the reactor coolant pipes is treated as a leak in a reactor coolant pipe.

If a leak occurs in a reactor coolant pipe or at the pressurizer, the coolant escaping through the leak accumulates in the containment sump.

In case of leakages occurring in the steam generator heating tubes, coolant from the reactor coolant circuit gets into the feedwater/steam circuit. Thus, coolant may also be released into the environment.

If a leak in a connecting pipe of the reactor coolant circuit outside the containment cannot be isolated, the water escaping from the pipe does not accumulate in the containment sump. If the leak occurs in a connecting pipe inside the annulus, consequential failures of the components located in the annulus and belonging to the emergency and residual heat removal system may result.

A leak in the pressurizer jacket as well as in the steam generator inlet or outlet headers is treated as a leak in the reactor coolant pipe. The same applies to small leaks in the reactor pressure vessel.

The following triggering events for transients and resulting accident sequences have been investigated:

- Failure of the reactor coolant supply,
- Failure of the main heat sink (turbine trip without opening of the main steam bypass system),
- Loss of preferred power (failure of the auxiliary power supply),
- Large and medium leak in a main steam pipe, (ATWS)[1]).

The investigations also covered loss-of-coolant accidents due to these transients during which the coolant escaped via pressurizer relief valves which by a mistake had remained in an open position.

Occurrence probabilities of triggering events as used in the Study are shown in detail in the first columns of Table 4-2 (loss-of-coolant) and Table 4-3 (transients) [see Section 4.3]. With respect to several loss-of-coolant accidents, Table 4-2 differentiates between the occurrence probability of a triggering event (e.g. the opening of a pressurizer valve) and the frequency of an event which initiates an accident (e.g. pressurizer valves remains open by/mistake).

In Phase B, the occurrence probabilities of operating transients as well as other operating data have been obtained throughout from the plant specific operating experience gathered in Unit B of the Biblis Nuclear Power Plant.

---

[1])"Anticipated Transients Without Scram (ATWS)" are understood to be event sequences from "transients to be anticipated" (occurrence probability greater than 10^2/a with an additional failure of the reactor scram system.

After completion of Phase A in 1979, a number of changes have been carried out at systems of the plant. Therefore, the operating experience gathered until 1979 could not be used for several triggering events. Thus, only the operating experience obtained since 1980 has been evaluated for the occurrence probabilities of the following triggering events:

- Failure of the main feedwater supply,
- Failure of the main heat sink, and
- Opening of pressurizer valves in the case of transients.

To determine, however, the probability of occurring a loss of preferred power, the entire operating time of the plant has been considered.

The occurrence probability of transients with a failure of the reactor scram system (ATWS) results as the product of the occurrence frequency for a transient and the failure probability for the reactor scram system with the latter having been determined by means of a reliability analysis.

Loss-of-coolant accidents are such rare events that their occurrence frequencies cannot be estimated with a sufficient degree of accuracy on the basis of plant specific operating experience.

In pressurized water reactors, no leaks have occurred so far in a coolant pipe which would have required the function of the emergency cooling systems. Therefore, the occurrence frequencies of small leaks (2–12 cm^2) in a reactor coolant pipe and of leaks in heat generator heating tubes (up to twice the cross section of a heating tube $\leqq$ 6 cm^2) have been estimated on the basis of German operating experience, although such a leak has not occurred up to now.

Similarly, the German operating experience has been used for the purpose of determining the frequencies of an inadvertent opening of pressurizer valves and of the inadvertently open position of either of the two isolating valves in an injection pipe of the emergency and residual heat removal system.

Frequencies of larger leaks in the pressure boundaries of the reactor coolant circuit can only be estimated theoretically. Due to the high quality standards of pipes of the reactor coolant circuit, the occurrence frequencies of medium and small leaks in a reactor coolant pipe or in outgoing sections of larger connecting pipes are extremely low. So, in fracture mechanical analyses a frequency of about 10^{-7}/a is estimated for the entire rupture of a larger pipe (double-ended rupture).

In order to determine the occurrence probabilities of medium and small leaks (with leak cross sections greater than 12 cm^2), and as a supplement to the operating experience, working hypotheses have been used quoting ratios for "leak before rupture" thus allowing a meaningful graduation of leak sizes in compliance with various nominal widths of pipes.

As far as the failure of the reactor pressure vessel is concerned, Phase A estimated an occurrence probability of less than 10^{-7} per reactor operating year. In Phase B this estimate was supplemented and further confirmed by an evaluation of recent research projects. A detailed discussion of this work is given in the technical report which is included in Section 4.5 of the Study [GRS 89]. Accordingly, a failure of the reactor pressure vessel can be ruled out as a risk-relevant accident pathway.

The occurrence frequencies of large and medium leaks in pipes of the main steam system have been estimated using the worldwide operating experience with pressurized water reactors and the data employed for pipe leaks in the US Reactor Safety Study WASH 1400. As far as leaks in pipes in the valve room are concerned, the same occurrence probability as for leaks in pipes of the reactor coolant circuit has been estimated after the valve room had been retrofitted to comply with the specifications of basic safety.

4.2 Thermohydraulic Analyses, Effectiveness Conditions for the Safety Systems

In order to be able to calculate the failure probabilities in event analyses, the minimum demands on the effectiveness must be known which have to be met by the safety systems. These minimum demands are understood as the requirements at least to be fulfilled by a system so that an accident is coped with. It specially has to be indicated how many of the multiple system legs in a system are required in order to fulfill the minimum requirements for a certain system function.

With respect to the requirements to be fulfilled by safety systems, the analyses carried out in Phase A had taken over the minimum requirements as laid down in the nuclear licensing procedure. In doing so, a core meltdown was already postulated in a simplified approach wherever the minimum requirements laid down by the licensing procedure could not be complied with. After completion of Phase A comprehensive research projects have been carried out for the analysis of accidents both at a national level and with international cooperation. So experiments were carried out at several test laboratories investigating in detail the thermohydraulic and fluid dynamic processes such as they occur in the course of loss-of-coolant accidents. In parallel with these investigations, efficient computer codes were developed for the simulation of accidents and then verified by a comparison with experimental results. By this work the knowledge about the sequence of accidents could be considerably extended and deepened. Today, it therefore is possible to far more precisely describe an accident than it could be done in Phase A.

In Phase B, comprehensive accident analyses have been carried out to determine the minimum requirements for the effectiveness of safety systems. According to the results of these analyses, the minimum requirements for coping with accidents are, in many cases, minor than those laid down in the nuclear licensing procedure.

So, for loss-of-coolant accidents, calculations covering the whole leak spectrum have been carried out with respect to leaks in a reactor coolant pipe. Table 4-1 includes the minimum requirements derived from these calculations for emergency cooling and residual heat removal.

Accordingly, one high-pressure and one low-pressure leg will be sufficient for the entire leak spectrum in order to cope with the accident. For leaks smaller than 200 cm^2, additional shutdown of the plant via the secondary side is required. In the case of occurring leaks with cross sections of more than 50 cm^2, the shutdown process must be initiated after 30 minutes at the latest. At leaks of less than 25 cm^2 cross sections, the reactor has to be shut down after two hours as a maximum. In the case of large and medium-sized leaks, the accumulators ensure a rapid refilling of the reactor pressure vessel. However, it is only in the range of medium leaks (i.e. 300 – 500 cm^2) that accumulators constitute a redundancy to the high-pressure injection system.

To leaks in a reactor coolant pipe apply the same minimum requirements as to leakages caused by open pressurizer valves. If one leg of the high-pressure injection is operable, the shutdown of the plant has to be performed at least 90 minutes after a leak of 20 cm^2 has occurred, and at least 45 minutes after having occurred a leak of 40 cm^2.

Detailed thermohydraulic analyses have also been carried out with respect to the effectiveness of the safety systems when occurring leaks in steam generator heating tubes. As a result of these analyses modifications in both the engineering of systems and the operating manual have been suggested which considerably improve the control of a leak in

Table4-1:
Minimum requirements for the effectiveness of the safety systems for emergency cooling and residual heat removal in the case of leaks in a reactor coolant pipe.

loss of coolant accident	leak cross section (cm^2)	system functions					feedwater supply	
		HP-safety injection	accumulator	LP-system flooding	LP-system sump re-circulation	permissible cooldown delay on sec. side (min)	systems	permissible delay for feed (min)
large leak	500	-	-	1	1	∞	-	∞
medium leak	200 - 500	1	-	1	1	∞	-	∞
	300 - 500	-	2	1	1	∞	-	∞
small leak	80 - 200	2	-	1	1	60		120
		1	-	1	1	30		90
	50 - 80	2	-	1	1	60		120
		1	3	1	1	60	1 HSW	120
		1	-	1	1	30	or	90
	25 - 50	2	-	1	1	90	2 NSW	120
		1	-	1	1	60		90
	2 - 25	1	-	1	1	60 (1ARV)		60
		1	-	1	1	120 (2ARV)		60
		-	-	1	1	30 (2ARV)		60
		1	-	1	1	120 (2ARV)	1 NSW	30

HSW: main feedwater
NSW: emergency feedwater
ARV: relief control valve

steam generator heating tubes. For a better understanding of these measures, in the following possible accident sequences are briefly described which may occur in the case of a heating tube leak.

When a heating tube leak occurs (which may be identified by measuring the activity at the main steam pipes), the reactor protection system automatically initiates countermeasures especially designed to cope with this accident. Following the reactor scram, pressurizer spraying and an automatic partial shutdown of the plant (50 K/h) lead to a rapid depressurization of the primary circuit and thus to a stabilization of the pressurizer level. As soon as the pressure falls below 8 MPa, the defective steam generator can be isolated without any response of the main steam safety valves and consequently without a loss of coolant via the secondary system.

In the case of heating tube leaks with a leak cross section of less than 6 cm^2, i.e. twice the cross section of a heating tube (double-ended rupture) the pressurizer level becomes stable after having attained the activation limit for emergency coolant injection.

In the case of larger leaks, e.g. if occurring a rupture of several heating tubes or an additional failure of the pressurizer spray system, the water level in the pressurizer falls so low that the activation criteria (emergency cooling criteria) for high-pressure safety injection are reached. If, in such a case, the high-pressure safety injection pumps would start, and in case they could not be stopped, an escape of coolant into the feedwater/steam circuit would result and ultimately an overfilling of the defective steam generator. The integrity of the main steam pipe would then be jeopardized by possible condensation effects and water loads. Similarly, a failure of main steam safety valves in open positions might occur.

Fig. 4-1 shows the different water levels in the defective steam generator and in the pressurizer, with the high-pressure safety injection system operating, in the case of occurring a double-ended rupture of a steam generator heating tube and an additional failure of the pressurizer spray system. From the figure it may be learned that, in the case of a heating tube rupture, approximately one hour is available in order to put the safety injection pumps out of service. In the case of several heating tube ruptures however, this time would become shorter due to the larger leak cross sections.

Thus, if the emergency criteria are reached in the case of a heating tube leak, the high-pressure safety injection is overridden by the reactor protection system. Furthermore, the cut-off can be effected at the con-

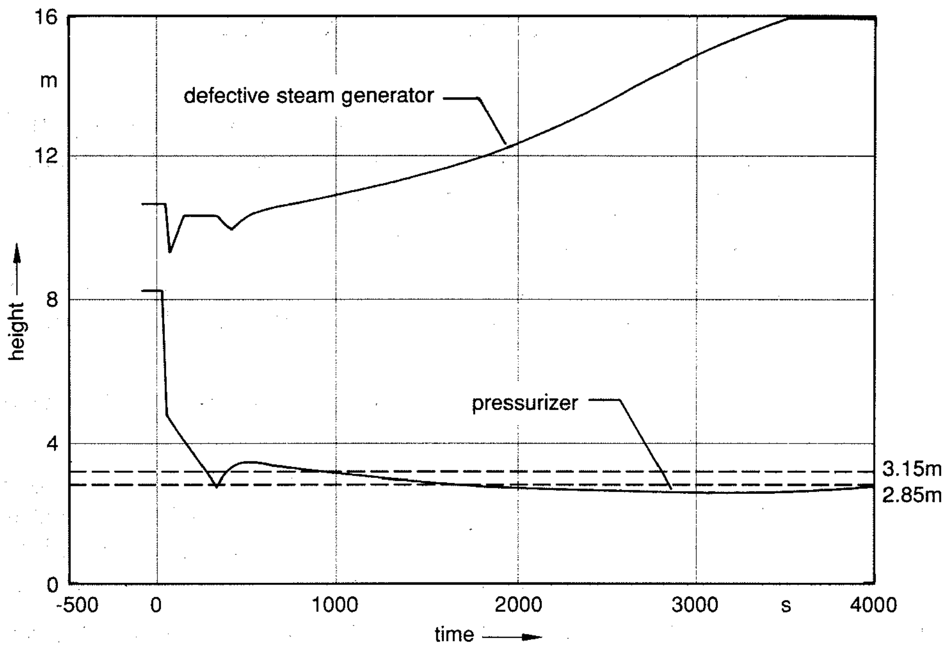


Fig. 4-1:
Water levels in a defective steam generator and in the pressurizer during a steam generator heating tube break (double-ended rupture) with failure of the pressurizer spray system.

trol room before the steam generator is completely filled and overfilled.

When occurring transients it is, as a rule, not necessary to shut the plant down at short notice. The heat can be removed via one of the four existing steam generators. If there is a lack of feedwater supply to the steam generators, these will steam out on the secondary side. The reactor coolant circuit is heated up, and the pressure increases to such an extent that one or more pressurizer valves open. The coolant then steams out at high pressure through the pressurizer valves. Core meltdown can be prevented if at least one of the steam generators is feeded again before the coolant level in the reactor pressure vessel falls below the top edge of the core. For this purpose, approximately one or to two hours are available, depending on the triggering event under review.

In order to cope with ATWS cases (operating transients with an additional failure of the reactor scram system), most cases require the opening of two out of three large pressurizer valves (each of them having an outlet cross section of 40 cm^2) if two of the four steam generators are fed.

4.3 Results of the Event Sequence Analyses

● **General Survey**

Tables 4-2 and 4-3 present the results of the systems reliability and event sequence analyses of loss-of-coolant accidents and transients investigated in Phase B. In detail are indicated:

- The frequencies of the triggering events,
- The conditional probabilities[1]) of a failure of the safety systems and/or system functions required for coping with the accident, and
- The frequencies of event sequences not coped with by the safety systems.

The frequencies of event sequences not coped with by the safety systems result from multiplying the occurrence frequencies of the respective triggering events by the conditional failure probabilities of the safety systems and/or system functions required to cope with the accident.

Table 4-4 includes further data relating to the results of the analyses. With respect to the failure probabilities of the systems needed for coping with the accident,

- the main contributions of various individual systems as well as
- the contributions of common cause failures and human failure

are quoted.

With respect to the occurrence frequencies of event sequences not coped with the following items are indicated:

- The frequency contributions derived from secondary and primary side failures, as well as
- The state of the plant [high pressure (HP), low pressure (LP)], associated with these contributions.

For high-pressure contributions

- the periods of time (in minutes) are quoted which are available as of the beginning of the accident in order to still prevent a core meltdown, or a core meltdown at high pressure (HP), by means of accident management measures.

[1]) Conditional means that the probability of failing the required system functions is determined under the conditions of the accident occurred. Thus, for example, the main steam bypass system is not available when failing the main heat sink.

Table 4-5 presents a summary of the results subdivided into LP and HP contributions. Finally, Table 4-6 compares the results of systems analyses with earlier results obtained in Phase A.

Fig. 4-2 provides a survey of the contributions of plant internal triggering events (event groups) to the frequency of event sequences not coped with (sum of the expected frequencies of injurious conditions) and to the therein included contributions of the failure probabilities of safety systems (contributions of the non-availabilities of the system functions).

• Discussion of the Results

All in all, the frequency of the event sequences of plant internal triggering events which are not coped with by the safety systems amounts to 2.6 10^{-5}/a. Here, the major contributions result from operating transients (approximately 60%) and from loss-of-coolant accidents via small leaks (approximately 25%), also see Fig. 4-2. Thus, in agreement with the results of Phase A, the leading contributions to the frequency of event sequences not coped with by system functions are determined by more frequent malfunctions which are "closely associated with operation".

For loss-of-coolant accidents, the major contributions result from the triggering events referred to as "small leak in a reactor coolant pipe (2 – 12 cm^2)" and "inadvertent opening of a pressurizer safety valve". The frequency of these events is determined by secondary side failures (approximately 65%) and primary side failures (approximately 35%). The share of common cause failures amounts to approximately 50%. Here, a significant contribution results from the failure of the level measurement in the borated water tanks which is necessary for changing over from emergency coolant injection to the sump recirculation mode of operation. The approximately 25% share which is due to human failure is mainly caused by the failure of intended manual interventions to initiate the shutdown of a plant.

For transients, the greatest contributions ($6.7 \cdot 10^{-6}$/a) is made by the simultaneous failure of the main feedwater supply and the main heat sink. This contribution is significantly determined by failures in which, following a pressure decrease in the main steam system, the activation of a signal for the isolation of the secondary circuit ($\Delta p/\Delta t$-signal) disconnects the main steam pipes from the common header and, at the same time, stops the main feedwater pumps.

Tab. 4-2:
Frequency of triggering events and accident sequences not coped with by safety systems for a loss of coolant accident

Nr.	triggering event for a loss of coolant accident	leak cross section (cm^2)	frequency (1/a) of initiating event	frequency (1/a) of triggering event	probability of system failure (1/demand)	frequency (1/a) of uncontrolled accident sequence
	<u>leaks in reactor coolant pipe</u>					
1	large and medium leak	> 200	$< 10^{-7}$		$< 3\cdot10^{-3}$	$< 10^{-8}$
2	small leak 1	80-200	$9{,}0\cdot10^{-5}$		$3{,}5\cdot10^{-3}$	$3{,}1\cdot10^{-7}$
3	small leak 2	50-80	$7{,}5\cdot10^{-5}$		$3{,}3\cdot10^{-3}$	$2{,}5\cdot10^{-7}$
4	small leak 3	25-50	$7{,}5\cdot10^{-5}$		$3{,}3\cdot10^{-3}$	$2{,}5\cdot10^{-7}$
5	small leak 4	12-25	$1{,}4\cdot10^{-4}$		$1{,}7\cdot10^{-3}$	$2{,}4\cdot10^{-7}$
6	small leak 5	2-12	$2{,}8\cdot10^{-3}$		$1{,}1\cdot10^{-3}$	$3{,}0\cdot10^{-6}$
	<u>leaks at pressurizer</u>					
	small leaks at pressurizer caused by transients					
7	· failure of main feedwater	20	$1{,}4\cdot10^{-1}$	$3{,}2\cdot10^{-5}$	$2{,}8\cdot10^{-3}$	$9{,}0\cdot10^{-8}$
8	· failure of main heat sink	20	$1{,}4\cdot10^{-1}$	$3{,}3\cdot10^{-5}$	$1{,}6\cdot10^{-2}$	$5{,}3\cdot10^{-7}$
9	· other transients	20	$5{,}3\cdot10^{-1}$	$1{,}2\cdot10^{-4}$	$1{,}7\cdot10^{-3}$	$2{,}0\cdot10^{-7}$
10	small leak at pressurizer due to inadvertent opening of safety valve	40	$2{,}0\cdot10^{-2}$	$8{,}5\cdot10^{-4}$	$2{,}6\cdot10^{-3}$	$2{,}2\cdot10^{-6}$
11	leak in connecting line to annulus	2-500	10^{-2} to 10^{-5}	$< 10^{-7}$	1	$< 10^{-7}$
	<u>leak in steam generator tube</u>					
12	small leak 1	6-12	$1{,}0\cdot10^{-5}$		$1{,}1\cdot10^{-2}$	$1{,}1\cdot10^{-7}$
13	small leak 2	1-6	$6{,}5\cdot10^{-3}$		$1{,}5\cdot10^{-4}$	$1{,}0\cdot10^{-6}$
1-13	frequency of uncontrolled accident sequences for loss of coolant accidents					$8{,}3\cdot10^{-6}$

Tabelle 4-3: Frequency of triggering events and accident sequences not coped with by safety systems during a transient

Nr.	event triggering a transient	frequency of triggering event (1/a)	probability of system failure	frequency of uncontrolled accident sequence (1/a)
	operating transients			
14	loss of preferred power	0,13	$1{,}7 \cdot 10^{-5}$	$2{,}2 \cdot 10^{-6}$
15	loss of main feedwater without loss of main heat sink (long-term)	0,15	$2{,}1 \cdot 10^{-5}$	$3{,}2 \cdot 10^{-6}$
16	loss of main feedwater and main heat sink	0,29	$2{,}3 \cdot 10^{-5}$	$6{,}7 \cdot 10^{-6}$
17	loss of main heat sink without loss of main feedwater	0,36	$8{,}0 \cdot 10^{-6}$	$2{,}9 \cdot 10^{-6}$
	transients caused by leaks in main steam line			
	large leak			
18	· within containment	$1{,}6 \cdot 10^{-4}$	$7{,}8 \cdot 10^{-3}$	$1{,}2 \cdot 10^{-6}$
19	· outside containment	$4{,}8 \cdot 10^{-4}$	$2{,}1 \cdot 10^{-3}$	$1{,}0 \cdot 10^{-6}$
	medium leak			
20	· within containment	$2{,}7 \cdot 10^{-5}$	$3{,}0 \cdot 10^{-3}$	$8{,}1 \cdot 10^{-8}$
21	· outside containment	$1{,}1 \cdot 10^{-4}$	$2{,}0 \cdot 10^{-3}$	$2{,}2 \cdot 10^{-7}$
	operating transients with failure of reactor scram (ATWS)			
22	ATWS during loss of main feedwater	$4{,}7 \cdot 10^{-6}$	$8{,}4 \cdot 10^{-3}$	$3{,}9 \cdot 10^{-8}$
23	ATWS during loss of preferred power	$3{,}4 \cdot 10^{-6}$	$2{,}3 \cdot 10^{-2}$	$7{,}8 \cdot 10^{-8}$
24	ATWS during loss of main heat sink and main feedwater	$7{,}5 \cdot 10^{-6}$	$5{,}0 \cdot 10^{-3}$	$3{,}8 \cdot 10^{-8}$
25	ATWS during other transients	$2{,}3 \cdot 10^{-5}$	$2{,}0 \cdot 10^{-3}$	$4{,}6 \cdot 10^{-8}$
14-25	frequency of uncontrolled accident sequences caused by transients			$1{,}8 \cdot 10^{-5}$

Tab. 4-4(1):
Non-availlability of system functions and frequencies of accident sequences not coped with by safety systems and caused by plant internal events (see also Tab. 10-5 in main vol. [GRS 89])

no. and type of triggering event	expected frequency / a (expected value)	non-availability of system functions: average	main contributions	percent %	% of causes of failure: CC %	MF %	expected frequency / a (point estimate) of plant damage states: SP	SP	SP	total
1. lge. + med leak in reactor coolant pipe (> 200 cm²)	< E-7	<3,E-3	LP injection	75	70	13		<E-8		<E-8
2. small leak 1 in reactor coolant pipe (80-200 cm²)	9,E-5	3,5E-3	LP injection MS relief	40 42	52	25	1,4E-7 LP	1,7E-7 LP		3,1E-7
3. small leak 2 in reactor coolant pipe (50-80 cm²)	7,5E-5	3,3E-3	LP injection MS relief	40 44	50	25	1,2E-7 LP	1,3E-7 LP		2,5E-7
4. small leak 3 in reactor coolant pipe (25-50 cm²)	7,5E-5	3,3E-3	LP injection MS relief	40 44	50	25	1,2E-7 60/85 HP	1,3E-7 30/40 HP		2,5E-7
5. small leak 4 in reactor coolant pipe (12-25 cm²)	1,4E-4	1,7E-3	LP injection MS relief	52 47	70	19	1,1E-7 60/85 HP	1,2E-7 120/135 HP	<E-8 60/85 HP	2,4E-7
6. small leak 5 in reactor coolant pipe (2-12 cm²)	2,8E-3	1,1E-3	LP injection MS relief HP-injec.∧ Shutdown	23 73 2	52	36	2,2E-6 60/85 HP	7,0E-7 240/260 HP	5,6E-8 60/85 HP	3,0E-6
7. small leak at pressurizer with loss of main feed-water (20 cm²)	3,2E-5	2,8E-3	LP injection feedwater failure HP-injec.∧ cooldown MS relief	32 40 3 25	45	36	5,8E-8 90/120 HP	2,9E-8 120/135 HP	<E-8 60/85 HP	8,8E-8
8. small leak at pressurizer with loss of main heat sink (20 cm²)	3,3E-5	1,6E-2	LP injection MS relief	6 94	60	31	5,0E-7 120/150 HD	3,0E-8 120/135 HD		5,3E-7

Tab. 4-4(2):
Non-availability of system functios and frequencies of accident sequences not coped with by safety systems and caused by plant internal events (first continuation)

no. and type of triggering event	expected frequency / a (expected value)	non-availability of system functions: average	main contributions	percent %	% of causes of failure: CC %	MF %	expected frequency / a (point estimate) of plant damage states: SP	SP	SP	total
9. small leak at pressurizer with other transients (20 cm²)	1,2E-4	1,7E-3	LP injection MS relief	52 47	70	19	9,1E-8 120/150 HP	1,1E-7 120/135 HP	<E-8 60/85 HP	2,0E-7
10. small leak at pressurizer due to inadvertent opening of safety valve (40 cm²)	8,5E-4	2,6E-3	LP injection MS relief	34 60	50	32	1,3E-6 90/120 HP	8,5E-7 45/60 HP		2,2E-6
11. leak in a connecting line in annulus	< E-7	1	emergency cooling	100	not analysed			< E-7 LP/HP		< E-7
12. leak in steam gen. tube (6-12 cm²)	1,0E-5	1,1E-2	not analysed	not analysed	not analysed	not analysed	not analysed 30/85 SG-HP	not analysed 30/400 SG-HP	not analysed 30/400 SG-HP	1,1E-7
13. leak in steam gen. tube (1-6 cm²)	6,5E-3	1,5E-4	steam gen. isol. ∧ leak refilling*) part. cooldown ∧ leak refilling *) shut off HP injec. loss of feedwater	38 13 13 38	26	68	3,7E-7 60/85 SG-HP	1,3E-7 60/650 SG-HP	5,0E-7 60/650 SG-HP	1,0E-6
14. loss of preferred power	0,13	1,7E-5	loss of feedwater	100	76	11	2,2E-6 120/150 HP			2,2E-6
15. loss of main feedwater w/o loss of main heat sink	0,15	2,1E-5	loss of feedwater	100	77	48	3,2E-6 70/95 HP			3,2E-6

Tab. 4-4(3):
Non-availability of system functios and frequencies of accident sequences not coped with by safety systems and caused by plant internal events (second continuation)

no. and type of triggering event	expected frequency / a (expected value)	non-availability of system functions					expected frequency / a (point estimate) of plant damage states			
		average	main contributions		% of causes of failure					
				percent %	CC %	MF %	SP	SP	SP	total
16. loss of main feed-water and main heat sink	0,29	2,3E-5	loss of feedwater	100	76	49	6,7E-6 80/105 HP			6,7E-6
17. loss of main heat sink w/o loss of main feedwater	0,36	8,0E-6	loss of feedwater	100	55	50	2,9E-6 80/105 HP			2,9E-6
18. large leak in MS line inside con-tainment	1,6E-4	7,8E-3	separation MS-system loss of feedwater	20 80	30	7	1,2E-6 70/95 HP			1,2E-6
19. large leak in MS line outside con-tainment	4,8E-4	2,1E-3	separation MS-system loss of feedwater	58 42	85	2	1,0E-6 70/95 HP			1,0E-6
20. medium leak in MS line inside con-tainment	2,7E-5	3,0E-3	separation MS-system loss of feedwater	40 60	63	5	8,1E-8 70/95 HP			8,1E-8
21. medium leak in MS line outside con-tainment	1,1E-4	2,0E-3	separation MS-system loss of feedwater	60 40	86	2	2,2E-7 70/95 HP			2,2E-7
22. ATWS during loss of main feedwater	4,7E-6	8,4E-3	loss of feedwater pressurizer valves	60 40	not anal.		2,4E-8 20/30 HP	1,5E-8		3,9E-8

Tab. 4-4(4):
Non-availability of system functios and frequencies of accident sequences not coped with by safety systems and caused by plant internal events (thirth continuation)

no. and type of triggering event	expected frequency / a (expected value)	non-availability of system functions					expected frequency / a (point estimate) of plant damage states			
		average	main contributions		% of causes of failure					
				percent %	CC %	MF %	$\underline{S}P$	$S\underline{P}$	$\underline{SP}$	total
23. ATWS with loss of preferred power	3,4E-6	2,3E-2	loss of feedwater pressurizer valves	98 2	not analysed	not analysed	7,5E-8 20/30 HP	< E-8 *)		7,8E-8
24. ATWS during loss of main heat sink and main feedwater	7,5E-6	5,0E-3	loss of feedwater pressurizer valves	90 10	not analysed	not analysed	3,4E-8 20/30 HP	< E-8 *)		3,8E-8
25. ATWS during other transients	2,3E-5	2,0E-3	loss of feedwater pressurizer valves	75 25	not analysed	not analysed	3,5E-8 20/30 HP	1,1E-8 *)		4,6E-8
sum, plant internal							2,3E-5 90,3 %	2,2E-6 8,8 %	2,3E-7 0,9 %	2,6E-5

*) This accident condition is not examined, since its total frequency is < 5,E-8/a

<u>Legend</u>

$\underline{S}$:	failure of secondary-side system functions
$\underline{P}$:	failure of primary-side system functions
$\underline{R}$:	failure of reactor scram
HP:	high pressure in primary circuit > 2 MPa
LP:	low pressure in primary circuit
t_1/t_2:	times (min) for prevention of core meltdown/prevention of HP case
PLR:	leak in the primary circuit in annulus
DE/SG:	steam generator
Λ:	and-connection
CC:	common cause failure
MF/HE:	human error

Table 4-5:
Frequency of accident sequences not coped with by safety systems and caused by plant internal events at low pressure (LP) and high pressure (HP)

no.	triggering events	frequency (1/a) of uncontrolled accident sequences LP	HP	total
	loss of coolant			
	leaks in reactor coolant pipe			
1-3	· leaks larger than 50 cm^2	$5{,}6\cdot10^{-7}$		
4-6	· leaks smaller than 50 cm^2		$3{,}5\cdot10^{-6}$	
7-10	leaks in pressurizer		$3{,}0\cdot10^{-6}$	
11	leak in connection line in annulus	$< 10^{-7}$	$< 10^{-7}$	
12-13	leaks in steam generator tube		$1{,}1\cdot10^{-6}$	
1-13	total loss of coolant	$6{,}6\cdot10^{-7}$	$7{,}6\cdot10^{-6}$	$8{,}3\cdot10^{-6}$
	transients			
14-17	operating transients		$1{,}5\cdot10^{-5}$	
18-21	transients caused by leaks in main steam line		$2{,}5\cdot10^{-6}$	
22-25	operating transients with failure of reactor scram (ATWS)		$2{,}0\cdot10^{-7}$	
	total, transients		$1{,}8\cdot10^{-5}$	$1{,}8\cdot10^{-5}$
1-25	grand total	$6{,}6\cdot10^{-7}$	$2{,}6\cdot10^{-5}$	$2{,}6\cdot10^{-5}$

Table 4-6:
Frequency of accident sequences not coped with by safety systems and caused by plant internal events, comparison of findings from Phase B and Phase A.

no.	triggering events	leak cross section (cm^2)	frequency (1/a) of uncontrolled accident sequences Phase B	Phase A [1]
	loss of coolant			
	leaks in reactor coolant pipe			
1	· large leaks	> 500	$< 10^{-8}$	$5,0\cdot10^{-7}$
	· medium leaks	200-500	$< 10^{-8}$	$2,0\cdot10^{-6}$
2	· small leaks	80-200	$3,1\cdot10^{-7}$	
3-6	· small leaks	2-80	$3,7\cdot10^{-6}$	$5,7\cdot10^{-5}$
	leaks at pressurizer			
7-9	· caused by opening of relief valve during transients	20	$8,2\cdot10^{-7}$	$9,0\cdot10^{-6}$
10	· caused by inadvertent opening of safety valve	40	$2,2\cdot10^{-6}$	
&				
11	leak in connection line in annulus		$< 10^{-7}$	$3\cdot10^{-8}$
12-13	leak in steam generator tube	1-12	$1,1\cdot10^{-6}$	
	transients			
	operating transients			
14	· loss of preferred power		$2,2\cdot10^{-6}$	$1,3\cdot10^{-5}$
15	· loss of main feedwater w/o loss of main heat sink (long-term)		$3,2\cdot10^{-6}$	$3,0\cdot10^{-6}$
16	· loss of main heat sink and main feedwater		$6,7\cdot10^{-6}$	$< 10^{-7}$
17	· loss of main heat sink w/o loss of main feedwater		$2,9\cdot10^{-6}$	
18-21	transients caused by leaks in main steam line		$2,5\cdot10^{-6}$	
	operating transients with failure of reactor scram (ATWS)			
22	· during loss of main feedwater		$3,9\cdot10^{-8}$	$6,0\cdot10^{-7}$
23	· during other transients		$1,6\cdot10^{-7}$	$7,0\cdot10^{-7}$
1-25	grand total		$2,6\cdot10^{-5}$	$8,6\cdot10^{-5}$

1) Shown in Phase A as contributions to frequency of core meltdown

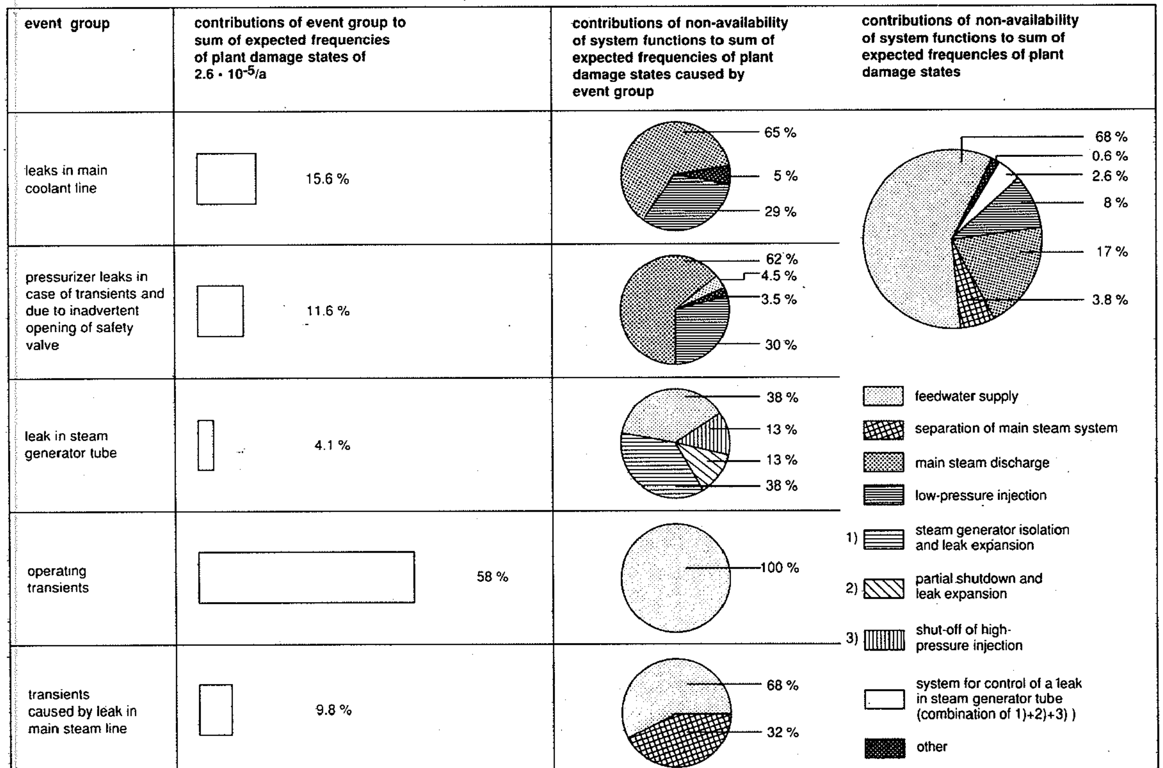


Fig. 4-2:
Plant internal triggering events
Contributions to the frequency of accident sequences not coped with by safety systems
(expected frequency of fault conditions)
Contributions of the non-availability of system functions

In almost all cases, sequences occurring during operating transients and not coped with are determined by a failure of the steam generator feeding. Here, the feeding of only one of the four steam generators by one system leg of the emergency feedwater system is already sufficient to remove the heat from the reactor. Therefore, the contribution of independent failures of individual system legs to the overall failure probability of the system is small. On the other hand, the share in the failure probability which is derived from common cause failures is relatively high. Therefore, the failure probability of the emergency feedwater systems is mainly determined by common cause failures of the emergency feedwater pumps and the associated auxiliary oil pumps.

Common cause failures of the emergency power diesels are only of importance if occurring a lengthy loss of preferred power in conjunction with a failure of the grid supply restoration.

The major shares of human failure are mainly failures of planned manual interventions which are required if the emergency feedwater system fails, in order to put the emergency system into operation (feeding from the adjacent Unit A).

Now as before only a very limited data base is available for the quantification of common cause failures. Thus, the assessment involves great uncertainties of estimation. Therefore, more differentiated evaluations of operating experience and investigations are needed for a better confirmation of common cause data. In addition, the share of human failures (failure of planned interventions), which is relatively high in certain event sequences, can be reduced by improved diagnostic aids and by an extended use of automated equipment.

Tables 4-4 and 4-5 show that practically all the accident sequences not coped with by system functions lead to a plant state which is characterized by high pressure (HP). Only loss-of-coolant accidents not coped with and with leak cross sections of more than 50 cm^2 lead to a plant state characterized by low pressure (LP), at a frequency of approximately 77/a (less than 3% of the total result).

- **Comparison with Phase A**

In Phase A, a core meltdown was already assumed, if for the effectiveness of the safety systems the minimal requirements laid down in the licensing procedures could not be met. Thus, the frequencies of event sequences not coped with, which are quoted for Phase A in Table 4-6, were equated with corresponding contributions to the frequency of core meltdowns. Thus, an overall frequency of $8.6 \cdot 10^{-5}/a$ resulted for core meltdowns in Phase A.

In the reliability analyses of Phase B, realistic minimum requirements for safety systems have been used as a basis (see Section 4.2). Moreover, the frequencies of event sequences not coped with by system functions and quoted in Table 4-6 with regard to Phase B, only correspond to contributions to the frequency of core meltdowns if, following the failure of the safety systems, no accident management measures are taken in order to restore core cooling and heat removal before a core meltdown occurs.

In Phase B a greater number of triggering events has been investigated than in Phase A. For the majority of the triggering events investigated in Phase A, Phase B revealed minor contributions to the frequency of event sequences not coped with by system functions. This results from numerous modifications of systems which have meanwhile been carried out after the completion of Phase A. In doing so, the formerly leading contributions in Phase A – i.e. the frequency of an uncontrolled small leak in a reactor coolant pipe and the frequency of an uncontrolled loss of preferred power – were both reduced by about one order of magnitude. The decisive aspects of these improvements were the installation of a partly automatic system for the controlled shutdown of the plant (100 K/h shutdown) in the case of small leaks as well as the possibility to supply power from the grid to safety-relevant loads (restoration of grid supply) after a failure of emergency power diesels.

As far as leaks in connecting pipes of the reactor coolant circuit were concerned, only rough estimates were made in Phase A. In Phase B, more detailed investigations have been carried out for these leaks. In doing so, an overall frequency of less than $10^{-7}/a$ has been determined for uncontrolled leaks in connecting pipes of the emergency and residual heat removal system.

Failures of the main feedwater supply together with a failure of the main heat sink, both of them caused by a response of the secondary circuit isolation, had not been taken into consideration in Phase A. The events which occurred during the first few operating years were interpreted as initial troubles not to be expected at comparable frequencies in future. The assessments made in Phase B are based on the operating experience gathered since 1980.

All in all, in Phase B, the frequency of event sequences which cannot be coped with by system functions is lower by a factor of three as compared with Phase A with respect to plant internal accidents. It amounts to 2.6 10^{-5}/a. Triggering events already investigated in Phase A account for about two-thirds of this value, i.e. a share of 1.7 10^{5}/a. Thus, results obtained for these event sequences have been definitely improved on the basis of the system modifications which have been performed since the completion of Phase A. The occurrence frequency is presently lower by a factor of about five.

Decisive contributions from the triggering events additionally investigated in Phase B result for those sequences which are not coped with and which originate from leaks on the pressurizer due to the inadvertent opening of a safety valve, the failure of the main heat sink and from leaks in the main steam system.

5. Fire, Flooding and External Impacts

5.1 Plant Internal Events

Fires and floods have been analyzed as spreading plant internal events. Details on the occurrence probabilities of important triggering events and resulting plant states not coped with are summarized in Table 5-1 and Fig. 5-1.

- **Fire**

The Study investigated such fires that may lead to a core meltdown as a consequence of failing engineered safeguards. In detail, sequences and consequences of fire have been simulated as a function of various fire protection measures and room temperature/time dependences.

The data used for the determination of the occurrence frequency of fires as well as for the reliability evaluation of fire protection measures are obtained from the operating experience at both nuclear and conventional power plants and are also used by property insurers and fire departments. The fire occurrence frequency determined for nuclear power plants in US statistics and amounting to 0.17 per year and plant has been taken over for the purposes of this Study. Similarly, US operating experience has been used to a great extent with respect to the fire occurrence frequencies in various compartment areas and with respect to the reliability data of fire protection measures.

The Study analyzed fires in various compartment areas. Fires inside the containment such as an oil fire in the area of the reactor coolant pumps and their oil supply systems, are limited as far as their propaga-

Tab. 5-1:
Frequency of triggering events and accident sequences not coped with by safety systems cused by fire, internal flooding and external impacts

no.	initiating/triggering events	frequency of triggering event (1/a)	probability of system failure (1/Anf)	frequency of uncontrolled accident sequence (1/a)
	<u>fire</u>			
26	failure of secured 220V d.c. power supply caused by fire in switching gear building	$2{,}5\cdot10^{-3} \times 1{,}6\cdot10^{-3}$ 1)	$4{,}2\cdot10^{-2}$	$1{,}7\cdot10^{-7}$
	<u>flooding of annulus</u>			
27	· when reactor is shut down (over 70cm)	$1{,}0\cdot10^{-3} \times 9{,}0\cdot10^{-4}$ 2)	$< 10^{-1}$	$< 10^{-7}$
28	· during power operation (over 90 cm)	$4{,}0\cdot10^{-3} \times 9{,}0\cdot10^{-4}$ 2)	$< 5\cdot10^{-2}$	$< 2\cdot10^{-7}$
	<u>external impacts</u>			
	transients caused by earthquake			
29	· intensity level 1	$7\cdot10^{-4}$	$1{,}0\cdot10^{-3}$	$7{,}0\cdot10^{-7}$
30	· intensity level 2	$9{,}5\cdot10^{-5}$	$2{,}0\cdot10^{-2}$	$1{,}9\cdot10^{-6}$
31	· intensity level 3	$5{,}0\cdot10^{-6}$	$8{,}1\cdot10^{-2}$	$4{,}0\cdot10^{-7}$
32	aircraft crash on reactor building	$6{,}3\cdot10^{-7}$	$< 0{,}15$	$< 10^{-7}$
26-32	total, fire, flooding and external impacts			$< 3{,}6\cdot10^{-6}$

1) probability of failing the fire protection measures

2) probability of failing annulus level measurement and line conversion

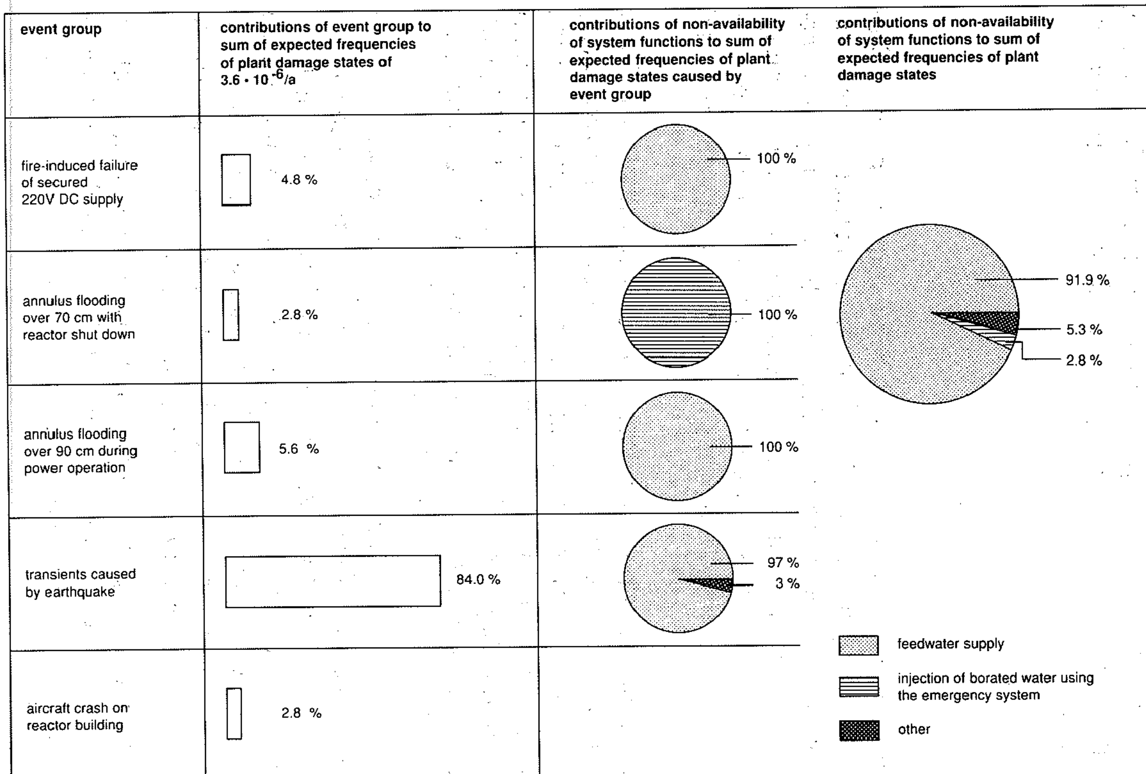


Fig. 5-1:
Fire, Flooding and External Events
Contributions to the frequency of accident sequences not coped with by safety systems
(expected frequency of plant damage states)
Contribution of non-availability of the system function.

tion and effects are concerned. Practically, they do not make any contribution to the frequency of core meltdowns.

Moreover, fires in various cable distribution systems and in the switchgear building have been analyzed. Here, the greatest contribution to the frequency of core meltdowns amounts to approximately $2 \cdot 10^{-7}$/a and results from an uncontrolled fire in the switchgear building. Under unfavorable conditions, such a fire causes the complete failure of the uninterruptible 220 V DC power supply. The resulting transient accident can still be coped with if supporting measures from the adjacent Unit A are taken to provide an emergency feedwater supply via the emergency system.

- **Flooding**

Plant internal flooding may cause the failure of components and thus malfunctions in the operation of the plant. Investigations show that above all a flooding of the annnulus of the reactor building may jeopardize the safety of the plant. The annulus accommodates safety-relevant components, such as equipment of the reactor protection system as well as the safety injection pumps of the emergency and residual heat removal system.

Flooding of the annulus is possible if a leak occurs in the service water system (the occurrence frequency of a large leak is approximately $5 \cdot 10^{-3}$/a). Decisive triggering events are maintenance errors or pipe ruptures. The service water system uses water from the River Rhine. If a service water pump delivers to full capacity (approximately 3000 t/h), flooding which may cause the failure of safety-relevant components must be expected within little less than 15 minutes.

Several backfitting measures have been taken in the plant which serve to improve the detection of leaks and to prevent flooding of the annulus. So, for example, the individual quadrants of the annulus, which are separated from each other by ground thresholds, are now monitored continuously by water level indicators. Thus, if a leak occurs, the defective leg of the service water system may be put out of operation before the thresholds of the respective quadrant are flooded.

As a result of the backfitting measures which have been taken, in total a very low occurrence frequency of less than $3 \cdot 10^{-7}$/a results for uncontrolled event sequences initiated by a leak in the service water system.

5.2 External Impacts

As far as external impacts are concerned, the Study analyzed in detail loads resulting from earthquakes. It further investigated the occurrence frequencies and effects of an aircraft crash. Details referring to the frequencies of these events and the resulting event sequences not coped with are again quoted in Table 5-1 and Fig. 5-1.

- **Earthquake**

For the determination of the seismic load assumptions, the macroseismic intensity has been chosen as a key parameter for the earthquake intensity. This quantity is characterized by an essentially closer link to the loads acting on and the damage caused to buildings than the free-field acceleration used formerly. Seismic engineering characteristics, in particular free-field response spectra and strong motion durations, have been determined as a function of intensities from a statistical evaluation of earthquake time histories recorded at sites with a subsoil similar to that at Biblis.

The seismic loads have been determined for selected buildings and components, and failure analyses have been performed for various parts and components. In doing so, mechanical components such as pumps and pipes of cooling systems, demineralized water tanks and the emergency diesels have been investigated with respect to their integrity, support stability and operability. A frequency of $3 \cdot 10^{-6}$/a has been determined for uncontrolled transients caused by earthquakes. The main contribution to this value results from a failure of the demineralized water tanks. If the demineralized water tanks fail, on a long-term basis the emergency feedwater system cannot be supplied with (demineralized) water.

Contributions from earthquake-conditioned loss-of-coolant accidents can be neglected.

- **Aircraft Crash**

Crash statistics of the past ten years have been used for the determination of the occurrence frequency of aircraft crashes. Here the statistics of fast flying military aircrafts are important. For the site of Biblis Nuclear Power Plant, a crash frequency of $9 \cdot 10^{-5}$/a km^2 was determined.

The loads acting on buildings which result from an aircraft crash depend on the mass of the aircraft, its crash velocity and its crash angle.

Frequency distributions determined for these influencing factors on the basis of crash statistics are used in order to determine the probability that the reactor building and other buildings of the plant are hit and that they fail. For this purpose, a Monte Carlo simulation method is used which is based on a physical modeling of the building and which mathematically simulates a great number of aircraft crashes.

For the frequency of an aircraft crash by which the reactor building is hit and penetrated, a value of approximately $1 \cdot 10^{-7}$/a results. In how far measures preventing a core meltdown are still possible in such a case has not been investigated. Hence, the determined frequency has been equated with that of a core meltdown.

The frequency of an aircraft crash upon the switchgear building is approximately $3 \cdot 10^{-7}$/a. In such a case, feeding of the steam generators can still be maintained via the emergency system (from Unit A). So, the frequency of an uncontrolled state of the plant is reduced to approximately $2 \cdot 10^{-8}$/a.

6. Accident Management Measures

6.1 Introduction

Based on the results of recent research projects in which the thermohydraulic processes during accidents have been subjected to closer analyses, comprehensive accident analyses have been carried out in Phase B. In doing so, the minimum requirements for the effectiveness of the Safety systems have been determined starting from very realistic assumptions. Above all, the analyses showed that in many cases, even after a failure of safety systems, accidents can still be coped with by accident management measures and a core meltdown can be prevented.

Results from analyzing plant internal accidents in terms of systems engineering show that the major contributions to event sequences not coped with for design reasons stem from transients and loss-of-coolant via small leaks. In many cases, the cause of the uncontrolled sequences is the failure of steam generator feeding. Thermohydraulic analyses show that these sequences initially involve slow changes of the conditions prevailing in the reactor coolant circuit. It therefore is still possible here, to prevent by accident management measures a melting of the fuel even after a failure of safety systems.

Accident management measures surpass the automatic and predetermined safety actions in that they comprise the flexible use of safety systems and operating systems which, in an emergency, take over failed safety functions. In this context, measures to prevent a core meltdown accident (accident prevention) are distinguished from measures to mitigate the consequences of an accident (accident mitigation).

Of particular importance are accident management measures which can prevent a core meltdown accident. The transition between these and the measures for coping with accidents is fluid. The last-named measures will be taken in the scope of the possibilities upon which the design of the safety systems is based. To a large extent those measures are included in the operating manual. Under aggravated conditions however, interventions by the operating personnel may be required which are not covered by the accident instructions. Therefore, accident management refers to further, and even preliminary measures which can still be taken in the case of safety systems should fail. As a rule, the requirements to be met by the systems, and in particular the requirements to be met by the operating personnel when implementing these measures, not only depend on the momentary situation, but also on the sequence of the accident concerned.

In the plant under review, a number of different and flexible possibilities exist in order to still prevent, or at least to delay, a core meltdown accident following a failure of safety systems. In a transient for example, which for design reasons is not coped with and during which the heat removal via the steam generators has failed, the high-pressure pumps of the volume control system can be used to compensate for the coolant steaming out through the pressurizer valves. In doing so, additional time will be saved to restore the heat removal via the steam generators before the water level in the reactor pressure vessel falls below the top edge of the core and core meltdown can start.

Some of the various possibilities of accident management have been reviewed in the Study. The following sections deal with mainly preventive accident management measures with respect to event sequences which cannot be coped with by system functions. Measures limiting the extent of damage are dealt with in Chapter 7 (Core Meltdown Accidents).

6.2 Measures Investigated

In a detailed approach, the Study dealt with measures which, following a depressurization of the reactor coolant circuit, are taken to restore core cooling and heat removal from the reactor before the fuel can begin to melt. These so-called bleed-and-feed measures can be initiated both in the feedwater/steam circuit on the secondary side and in the reactor coolant circuit on the primary side.

- **Measures on the Secondary Side**

If the water level in the steam generators falls below 2 m, the secondary system can be depressurized to a pressure below 1 MPa by opening the main steam relief valves or also the safety valves. The steam generators can then be fed either with water from the feedwater tank (passive mode) or by means of mobile pumps (active mode), e.g. fire fighting pumps. The residual heat is removed via the main steam relief system into the environment.

- **Measures on the Primary Side**

Apart from the measures on the secondary side, direct interventions on the primary side are also possible in order to relieve the high pressure in the reactor coolant circuit. For this purpose, the pressurizer valves are opened. In doing so, the pressure in the reactor coolant circuit is decreased to such an extent that, below 11 MPa, the high-pressure injection pumps feed emergency water and cool the reactor core again. If the pressure falls below 2.6 MPa, the accumulators start feeding as well. In case the pressure falls below 0.9 MPa, the residual heat can be removed via the residual heat removal system.

Measures on the primary side are only taken if measures on the secondary side are impossible or have failed. Measures on the primary side have to be initiated at the latest when the level in the reactor pressure vessel falls below the lower edge of the nozzle of the reactor coolant pipe. The depressurization on the primary side should also be initiated as soon as the fuel element outlet temperature is higher than 400° C or if the shutdown of the plant at 100 K/h is not successful in case a loss-of-coolant accident occurs.

- **Goals and Implementation of the Measures**

With these measures the following goals can be reached:

- Depressurization and feeding on the secondary side can restore heat removal via the steam generators so that the core is cooled sufficiently.
- Sufficient core cooling can also be reached by depressurization on the primary side if, with descreasing pressure in the primary system, high-pressure safety injection is initiated and the reactor core is filled again.
- If the high-pressure safety injection is not available, e.g. in the case of a complete failure of energy supply (station blackout), time may be gained with accumulator feeding in order to restore safety functions which have failed, e.g. energy supply, before a core meltdown sets in.
- If a core meltdown sets in, depressurization of the primary system will prevent meltdown at high pressure.

To perform these measures on the secondary and primary side, the following modifications are carried out at the plant:

- Modifications in the reactor protection system,
- Modifications which permit a depressurization and automatic feeding of the steam generators from the feedwater tank,
- The installation of additional connections for mobile pumps on the pressure side of the emergency feedwater pumps,
- The installation of a water level probe in the upper plenum of the reactor pressure vessel,
- The design of the pressurizer valves and the associated control valves to enable the relief of water/steam mixtures (two-phase mixtures). For these purposes, the pressurizer relief valves and the safety valves are provided with an additional control pipe which can be opened by motorized valves. The motorized valves in turn will be provided with a power supply secured by independent batteries.

6.3 Effectiveness of the Measures Investigated

Thermodynamic analyses have been carried out to determine the effectiveness of measures taken and, above all, the available periods of time.

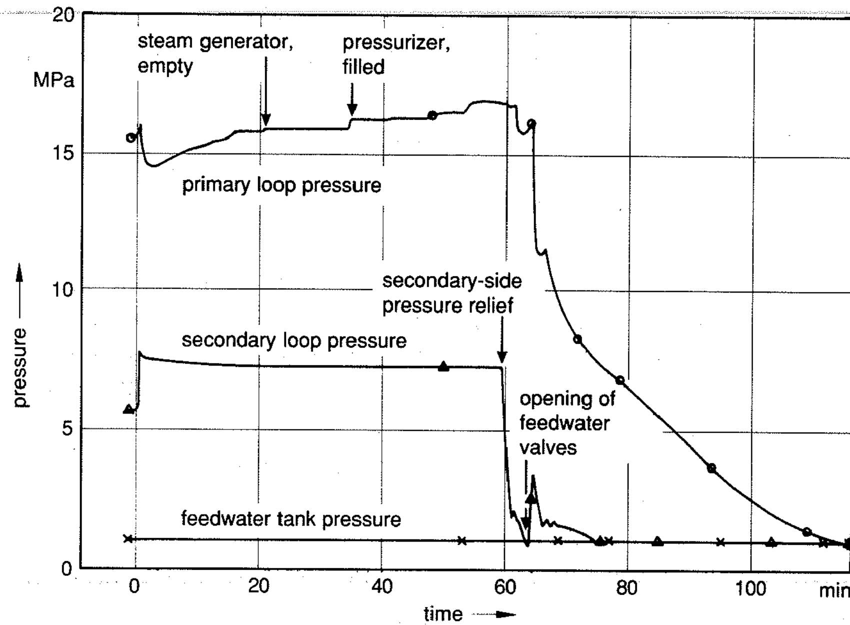


Fig. 6-1:
Pressure in primary and secondary systems during transient "failure of the main feedwater supply" with additional failure of emergency feedwater supply and secondary-side accident management measures.

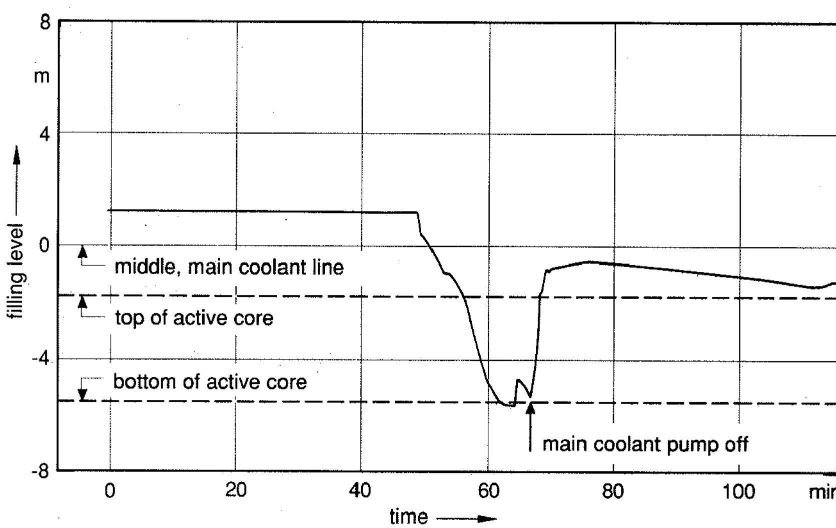


Fig. 6-2:
Water level curve in reactor pressure vessel during transient "failure of the main feedwater supply" with additional failure of emergency feedwater supply and secondary-side accident management measures.

Figs. 6-1 and 6-2 show the results of some calculations concerning measures taken on the secondary side. A "failure of the main feedwater supply system" is assumed as triggering event. Furthermore, it is assumed that steam generator feeding has failed completely, i.e. neither the emergency feedwater system nor the emergency system are available.

Fig. 6-1 shows the pressure history in the primary and secondary systems during the above event with a depressurization initiated on the secondary side 60 minutes after the accident has set in.

If feeding is not available, the steam generators will have dried out already after 20 minutes. The energy input from the reactor coolant pumps which continue to operate, further accelerates the steaming out of the steam generators. Subsequently, the reactor coolant circuit is heated up and the two relief valves on the pressurizer respond. Water escapes through the relief valves, as the pressurizer is completely filled with water.

Depressurization on the secondary side is initiated 60 minutes after the onset of the accident (Fig. 6-1). When the main steam relief valves are opened, the pressure in the feedwater/steam circuit decreases very fast. After the opening of the feedwater valves, water from the feedwater tank gets into the empty steam generators.

The secondary-side measures directly lead to a decrease of the pressure on the primary side. The pressurizer valves close. About 10 minutes after the depressurization has set in, the pressure in the primary system falls below 11 MPa. The primary circuit is filled again by the high-pressure safety injection. In case of failing the high-pressure safety injection system, the pressure in the reactor coolant circuit will have decreased to the feeding pressure of the accumulators about 30 minutes later.

Fig. 6-2 shows the corresponding coolant level in the reactor pressure vessel[1]). After the opening of the pressurizer valves the coolant level in the reactor pressure decreases. At the time of depressurization on the secondary side (at 60 min), the coolant level has fallen to the bottom edge of the core. Feeding of the steam generators must be effected at the latest at this time in order to avoid a core heatup that could no longer be stopped.

---

[1]) The coolant level in a certain volume area is a measure of the entire water inventory contained in the volume area, e.g. in a coolant/steam mixture.

The reactor coolant pumps which continue to operate at first still provide adequate core cooling. They are stopped automatically only when the emergency cooling signal for high-pressure safety injection is received (after about 65 min).

With the high-pressure safety injection not available, core cooling is ensured even after the reactor coolant pumps run down, since the beginning separation of water and steam effects a reincrease of the water inventory in the core. The coolant level in the reactor pressure vessel again rises above the top edge of the core. Heat removal from the core is effected in the natural circulation mode. The steam rising from the core area condenses in the heating tubes of the steam generators, the condensate flows back and accumulates again in the lower areas of the reactor coolant circuit (reflux condenser mode).

Considering the same case, Fig. 6-3 shows calculations concerning measures on the primary side. The pressure in the primary system and, as a measure of the water inventory in the core and in the upper plenum of the pressure vessel, the corresponding filling level histories have been plotted. One hour after the accident has set in, the water level in the upper plenum has sunk to the bottom edge of the reactor coolant pipe. At this time the primary measure (opening of the first and of the second pressurizer relief valve) is taken.

At the same time, the reactor coolant pumps are stopped automatically. This means that the cooling conditions for the core are getting worse. The coolant level decreases and reaches the bottom edge of the reactor core when high-pressure safety injection sets in (after approximately 70 min). For fuel rods with an average heat flux, maximum cladding tube temperatures of 700 °C result at that time. Subsequently, the high-pressure safety injection pumps start feeding. About 75 minutes after the beginning of the accident, the reactor pressure vessel is again sufficiently refilled.

According to the results of these analyses, a "failure of the main feed-water supply" which is not coped with by safety system functions must be followed by measures on the secondary or primary side at the latest one hour after the accident has begun in order to restore core cooling. For other transients not coped with by system functions, longer periods of time are available, e.g. at least two hours in the event of an uncontrolled loss of preferred power.

Calculations for loss-of-coolant accidents show that the admissible periods of time to restore core cooling and residual heat removal in the

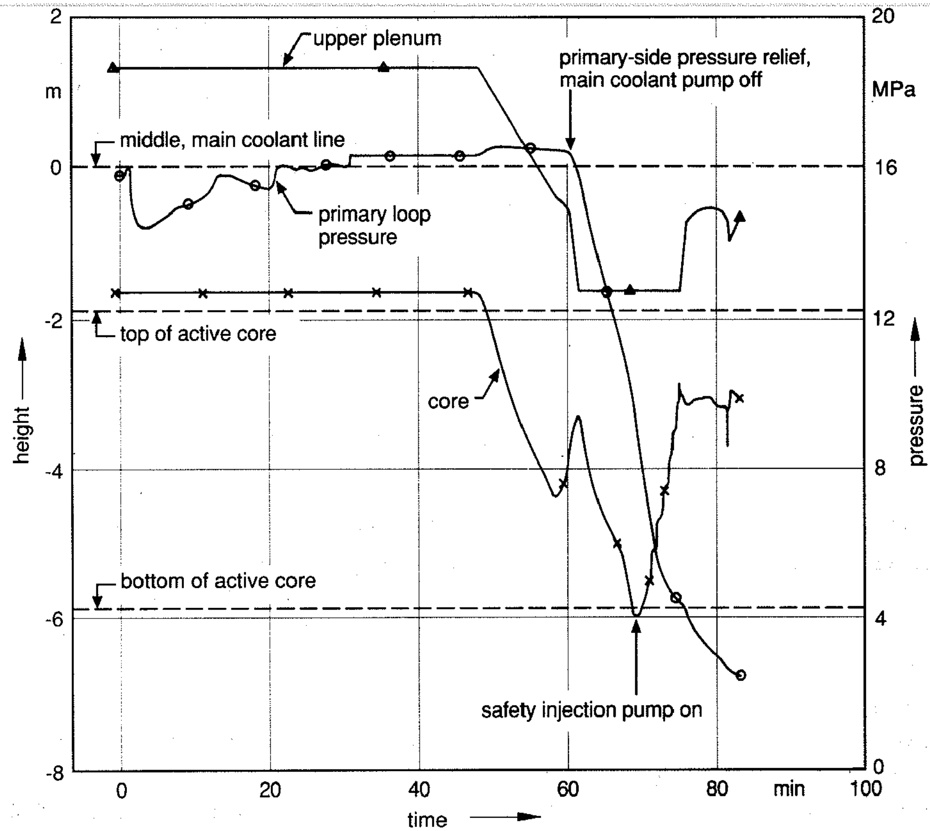


Fig. 6-3:
Pressure and level curves in primary system during transient "failure of main feedwater supply" with additional failure of emergency feedwater supply and primary-side accident management measures.

case of uncontrolled event sequences initiated by small leaks (< 25 cm²) amount to about 60 minutes for failures on the secondary side and to about 120 minutes (12–25 cm²) or 240 minutes (2–12 cm²) for failures on the primary side (see Table 4-4).

If core cooling and residual heat removal cannot be restored by means of these measures, a core meltdown sets in. Even in such a case, however, a core meltdown at high pressure is prevented by the opening of pressurizer valves. The accident sequence is transferred to conditions at low pressure (LP*) before bigger parts of the core melt and the reactor pressure vessel fails.

In order to avoid core meltdown at high pressure, the times available for depressurization measures on the primary side are longer than those for the restoration of core cooling and residual heat removal.

They amount for example, to about 95 minutes from the beginning of the accident when occurring a failure of the main feedwater supply not to be coped with by safety systems. Further data concerning the latest possible times for a primary side depressurization in order to prevent a core meltdown are compiled in Table 4-4.

6.4 Evaluation of the Measures Investigated

The details of these measures and associated procedures as well as the instructions to the operating personnel are being prepared and laid down by the licensee. Therefore, upon completion of the Study, detailed documents for individual and final assessments were not yet available. Thus, they have been assessed in the Study on a preliminary basis only.

The estimates performed are included in Table 6-1. The frequencies of uncontrolled event sequences without and with consideration of accident management measures (AM) are compared and subdivided into plant states referred to as LP, LP* and HP. LP* denotes a plant state where a core meltdown cannot be prevented, core meltdown at high pressure can be avoided however, by depressurization of the primary circuit.

If measures on both the secondary and the primary side are possible to restore the core cooling, they are assumed to be successful in 99 out of 100 cases (failure probability of 10^{-2}). With respect to event sequences with more unfavorable plant or time conditions the probabilities of success are assumed to be smaller.

Loss-of-coolant accidents involving leaks greater than 50 cm^2 and not coped with by system functions lead to a core meltdown at low pressure (LP). For these sequences, which rapidly result in a core meltdown, current planning does not provide for accident management measures.

Loss-of-coolant accidents not coped with and involving leaks smaller than 50 cm^2 would similar to transient sequences lead to a core meltdown at high pressure (HP) if countermeasures not have been taken in time. Here, the contribution of safety system failures on the primary side (emergency core cooling) amounts to about 35%. With respect to

Table 6-1:
Frequency of uncontrolled accident sequences, without and with consideration of accident management measures (AM).

no.	triggering events	frequency (1/a) without AM LP	frequency (1/a) without AM HP	frequency (1/a) with AM LP	frequency (1/a) with AM LP*	frequency (1/a) with AM HP
	loss of coolant					
	leaks in reactor coolant pipe					
1-3	· leaks larger than 50 cm²	$5{,}6\cdot10^{-7}$		$5{,}6\cdot10^{-7}$		
4-6	· leaks smaller than 50 cm²		$3{,}5\cdot10^{-6}$		$1{,}0\cdot10^{-6}$	$3{,}5\cdot10^{-8}$
7-10	leaks in pressurizer		$3{,}0\cdot10^{-6}$		$1{,}0\cdot10^{-6}$	$3{,}0\cdot10^{-8}$
11	leak in connection line in annulus	$< 10^{-7}$	$< 10^{-7}$	$< 10^{-7}$		
12-13	leaks in steam generator tubes		$1{,}1\cdot10^{-6}$		$1{,}3\cdot10^{-8}$	$1{,}1\cdot10^{-8}$
1-13	total, loss of coolant	$6{,}6\cdot10^{-7}$	$7{,}6\cdot10^{-6}$	$6{,}6\cdot10^{-7}$	$2{,}0\cdot10^{-6}$	$7{,}6\cdot10^{-8}$
	transients					
14-17	operating transients		$1{,}5\cdot10^{-5}$		$3{,}0\cdot10^{-8}$	$1{,}5\cdot10^{-7}$
18-21	transients caused by leaks in main steam line		$2{,}5\cdot10^{-6}$		$< 10^{-8}$	$2{,}5\cdot10^{-8}$
22-25	operating transients with failure of reactor scram (ATWS)		$2{,}0\cdot10^{-7}$		$2{,}0\cdot10^{-8}$	$2{,}0\cdot10^{-8}$
14-25	total, transients		$1{,}8\cdot10^{-5}$		$6{,}0\cdot10^{-8}$	$2{,}0\cdot10^{-7}$
1-25	total, plant internal accidents	$6{,}6\cdot10^{-7}$	$2{,}6\cdot10^{-5}$	$6{,}6\cdot10^{-7}$	$2{,}1\cdot10^{-6}$	$2{,}7\cdot10^{-7}$
	external events					
26	fire		$1{,}7\cdot10^{-7}$		$1{,}7\cdot10^{-7}$	$< 10^{-8}$
	flooding of annulus					
27	· with reactor shutdown	$< 10^{-7}$		$< 10^{-7}$		
28	· during power operation		$< 2\cdot10^{-7}$		$< 2\cdot10^{-7}$	$< 10^{-8}$
29-31	transients caused by earthquake		$3{,}0\cdot10^{-6}$		$9{,}0\cdot10^{-8}$	$9{,}0\cdot10^{-8}$
32	aircraft crash		$< 10^{-7}$			$< 10^{-7}$
26-32	total, external events	$< 10^{-7}$	$3{,}5\cdot10^{-6}$	$< 10^{-7}$	$4{,}6\cdot10^{-7}$	$< 2{,}0\cdot10^{-7}$
1-32	grand total	$7{,}6\cdot10^{-7}$	$2{,}9\cdot10^{-5}$	$7{,}6\cdot10^{-7}$	$2{,}5\cdot10^{-6}$	$4{,}5\cdot10^{-7}$

this contribution, depressurization on the primary side can only prevent HP core meltdown[1]). The event sequences will then lead to a core meltdown at low pressure (LP*). When occurring event sequences which involve failures on the secondary side (approximately 65%), accident management will in most cases prevent a core meltdown.

[1]) For small leaks with failures on the primary side, in any case a primary-side bleed (opening of two pressurizer valves) is required in order to prevent a high-pressure core meltdown. A timely bleed and feed however, may considerably defer the point of time at which primary-side action has to be taken.

event group	contribution to LP and LP* core meltdown frequency	
leaks in main coolant line	50%	expected frequency of all plant damage states: $2.9 \cdot 10^{-5}$/a
pressurizer leaks induced by transients and inadvertent opening of safety valves	32%	expected frequency of all core meltdown accidents (LP and LP* and HP): $3.6 \cdot 10^{-6}$/a
fire, internal flooding	14%	expected frequency of all LP and LP* core meltdown accidents: $3.2 \cdot 10^{-6}$/a (88%)
earthquake induced transients	2.8%	
other	1.2%	

Fig. 6-4:
Contributions of individual event groups to the frequency of low-pressure core meltdown accidents (LP and LP[1])).

In the case of occurring a leak up to 6 cm^2 in a steam generator heating tube a further escape of coolant into the feedwater/steam circuit can be prevented, even under the assumption that the heat removal on the secondary side should fail if depressurization on the primary side is effected after 60 minutes at the latest.

In most cases, uncontrolled plant states due to transients are caused by a failure of steam generator feeding. Core cooling and heat removal can be restored by measures on both the secondary and the primary side. After depressurization on the primary side, as a rule, the high-pressure and low-pressure injections of the emergency core cooling systems are available in order to prevent a core meltdown.

Accident management measures are also possible in the case of spreading events (fire, flooding, external impacts). Their probable success or their influence on the frequency of a core meltdown has been estimated. So, for the case of occurring uncontrolled event sequences resulting from a flooding in the annulus by which a core meltdown at high

event group	**contribution to HP core meltdown frequency**	
leaks in main coolant line	7.7%	expected frequency of all plant damage states: $2.9 \cdot 10^{-5}$/a; 97.8% under high press.
leaks in pressurizer during transients and induced by inadvertent opening of safety valve	6.7%	expected frequency of core meltdown accidents (LP and LP* and HP):
operating transients	33%	expected frequency of all core meltdown accidents under high pressure: $4.5 \cdot 10^{-6}$/a (12.5% of all core melt-down accidents or 1.5% of all HP plant damage states
transients caused by leaks in main steam line	5.7%	
external impacts (earthquake and aircraft crash)	41%	
operating transients with failure of reactor scram	3.7%	

Fig. 6-5:
Contributions of individual event groups to the frequency of high-pressure core melt-down accidents (HP).

pressure shall be prevented, a failure probability of $3 \cdot 10^2$ has been assumed for depressurization on the primary side. Similarly, e.g. at a power supply failure due to an earthquake, depressurization on the primary side can prevent core meltdown at high pressure, as the pressurizer relief and safety valves may be opened and kept open by means of battery-powered control valves.

The results considering accident management measures are presented in Figures 6-4 and 6-5. Accident management measures reduce the frequency of a core meltdown by one order of magnitude, i.e. from $2.9 \cdot 10^{-5}$/a to $3.6 \cdot 10^{-6}$/a. Thus, almost 90% of all the cases are coped with, and a core meltdown is prevented. In about 10% of the cases, a core meltdown cannot be prevented, but it is only in approximately 1.5% of all cases that a core meltdown at high pressure results.

7. Core Meltdown Accidents

7.1 Accident Sequences under Review

If an accident is not coped with by the safety systems available in the plant, and if core cooling cannot be restored in time by accident management measures, a core meltdown will result.

The processes involved in a core meltdown accident and the associated phenomena and loads are complex. In detail have to be investigated:
- the processes when melting the fuel in the reactor pressure vessel,
- the processes following a failure of the reactor pressure vessel, and
- the behavior of the containment.

The investigations concerning core meltdown accidents are based on findings of national and international reactor safety research, and in particular on results of research projects carried out in the scope of the German core meltdown program for-light water reactors. Here, the results of recent research projects and of additional investigations carried out in the Study have led to evaluations which differ in a number of issues from older assessments.

The Study considers various accident sequences. The following cases are distinguished:

Core meltdown at low pressure (LP)

Core meltdown at low pressure sets in when failing the emergency core cooling systems in the case of a loss-of-coolant through a larger leak in the reactor coolant circuit. The steam escaping through the leak into the containment causes a rapid pressure relief in the reactor coolant circuit. However, as the core is not cooled, melting at low pressure sets in.

Core meltdown at high pressure (HP)

Core meltdown at high pressure is possible if, following a transient accident or a loss-of-coolant through a small leak, heat removal via the steam generators fails entirely for a longer period of time and the reactor remains under high pressure. The reactor coolant circuit will not be relieved before the reactor pressure vessel fails after the meltdown of the core.

Core meltdown at low pressure following a depressurization of the reactor coolant circuit (LP)*

With a depressurization on the primary side, accident sequences which are first initiated at high pressure are transferred to conditions under low pressure (LP*) before the reactor pressure vessel fails after the meltdown of the core.

Core meltdown sequences with a bypassing of the containment

In the case of core meltdown sequences resulting from

- a steam generator heating tube leak not coped with and
- the rupture of a residual heat removal pipe in the annulus,

fission products may be released into the environment of the plant whilst bypassing the containment.

For core meltdown resulting from an uncontrolled leak of steam generator heating tubes, it has been assumed that the high-pressure safety injection cannot be cut off so that the steam generator is overfed. In such a case, core cooling is only ensured as long as the coolant reserves in the borated water storage tanks are not exhausted.

If core meltdown cannot be avoided when occuring a heating tube leak, core melting under high pressure (HP) is prevented if the pressure in the reactor coolant circuit is decreased by an opening of pressurizer valves, and the accident sequence is transferred into core meltdown at low pressure (LP*).

A very low occurrence frequency ($< 10^{-7}$/a) has been estimated for the rupture of a residual heat removal pipe in the annulus. Such a rupture can only occur in case the two-fold isolations from the reactor coolant circuit fail which are provided in the residual heat removal pipe. In such a case, it has to be assumed that the pumps of the emergency core cooling and residual heat removal system which are located in the annulus will not operate because of the thermal stress and the high humidity level. The only thing that happens is an injection of emergency core cooling water from the accumulators into the pressure vessel. As soon as this water has steamed out, the core heats up to melting temperature.

Table 7-1 indicates periods of time until the onset of core meltdown and the failure of the reactor pressure vessel for the core meltdown sequences investigated.

In the course of a core meltdown accident, various phenomena and processes occur which may have different effects upon the containment. In this context, the following sections deal with the loads acting on and the behavior of the containment with respect to

Table 7-1:
Timing data relating to core meltdown accidents (minutes after onset of the accident)

core meltdown	onset of core meltdown (min)	failure of reactor pressure vessel (min)
core meltdown LP	55	120
core meltdown HP	110	140
core meltdown LP* after primary bleed	330	410
core meltdown after		
• uncontrolled leak in steam generator tube (12 cm^2), after primary bleed	540	710
• uncontrolled leak of residual heat removing line in annulus	80	140

- a steam explosion,
- a failure of the reactor pressure vessel,
- a hydrogen combustion and
- the interaction between concrete and molten mass.

7.2 Steam Explosion

If molten mass gets into contact with water, the latter may steam out instantaneously and thus cause a pressure surge. This process is referred to as steam explosion. The intensity of the pressure surge depends on which percentage of the heat stored in the molten mass is converted into the mechanical energy of the pressure surge. For a core meltdown at low pressure, it has been analyzed whether or not a steam explosion can occur which jeopardizes the containment vessel.

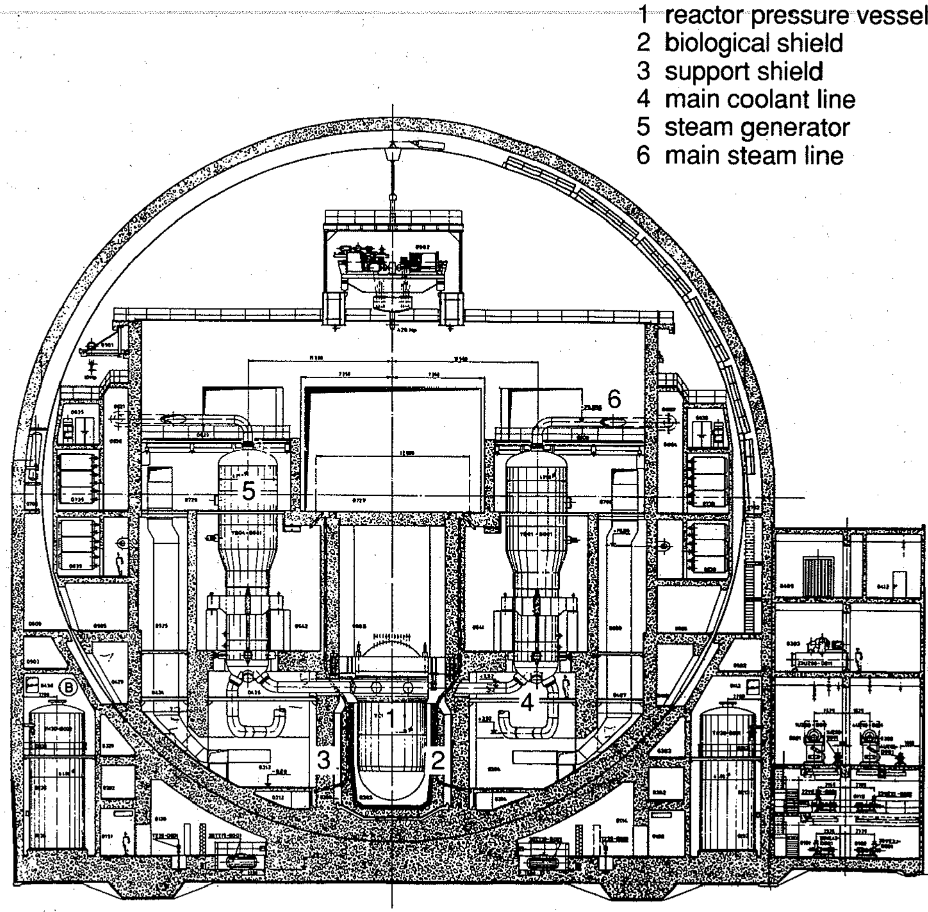


Fig. 7-1:
Containment with internals (scale approximately 1:600)

A steam explosion may occur if, towards the end of the core heatup and core destruction phase, molten core material slumps into the water still available in the bottom head of the reactor pressure vessel (Fig. 7-1). The pressure surge caused by the instantaneous steaming out of the water may destroy the pressure vessel and thus, at the same time, jeopardize the containment.

The occurrence of a steam explosion in the pressure vessel depends on the simultaneous fulfillment of various conditions:

- The molten mass involved in the reaction must be sufficiently large [molten mass quantity condition].

- The heat transfer between molten mass and water must be extraordinarily intensive. This is only possible if the molten mass is fragmented into very small particles (diameter of 10^{-3} – 1 mm) [contact surface condition]. This fine fragmentation must happen within an extremely short period of time (a few hundredths of seconds) in order to achieve a simultaneous reaction of the masses involved [coherence condition].
- The intensive heat transfer between molten mass and coolant must prevail sufficiently long so that an adequate amount of energy is transferred to the coolant for instantaneous flashing [contact time condition].

Only a rough estimate can be made with respect to the amount of molten mass that slumps into the residual water quasi-simultaneously with the failure of the lower core support structures. In this context, the way of failing the core support structure with the fuel element end plates is the decisive aspect. As a rule, a local failure of individual end plates has rather to be expected than the simultaneous failure of several end plates. Estimates of the possible discharge areas show that the failure of a single fuel element end plate may cause a molten mass of between some 100 kg to a maximum of 3000 kg to flow into the water within a few seconds.

An important parameter for the assessment of the interaction between molten mass and coolant is the degree of energetic conversion, the ratio between the mechanical energy released into a pressure surge during the interaction and the thermal energy of the molten mass involved. Besides theoretical approaches, a number of experimental investigations have been carried out in this context.

For experiments with molten masses in the kg order of magnitude, both simulation materials and real core meltdown materials have been used. In general, conversion degrees of a few percent (up to approximately 3%) have been found, in some cases up to approximately 17% for simulation materials.

In a core meltdown accident, the conditions for mixing processes and fragmentation may be less favorable than in an experiment. With an increasing quantity of molten mass the share of core melt diminishes, that finely fragmented can react with the coolant. A steam explosion involving a coherently fragmented molten mass of several 1000 kg and a conversion degree of up to 10% is unlikely.

Nevertheless, the Study carried out calculations in which a steam explosion under unfavorable conditions has been postulated and the resulting loads acting on the reactor pressure vessel have been estimated. In doing so, a thermal energy of 15 000 MJ has been assumed; this corresponds to a molten mass of about 10 000 kg participating in the reaction. Moreover, a conversion degree of 10% has been assumed for the conversion into mechanical energy. According to the results of these calculations, the highest loads caused by the pressure surge are observed in the spherical segment of the bottom head. These loads do not lead to a failure of the reactor pressure vessel.

On a whole the assessments show that due to the present state of knowledge a violent steam explosion simultaneously destroying both the reactor pressure vessel and the containment can be ruled out as a risk relevant accident pathway.

7.3 Failure of the Reactor Pressure Vessel

During a core meltdown the progressive destruction of the reactor core also includes the failure of the core support structures. Greater shares of core melt and molten structural materials drop into the bottom head of the pressure vessel. The residual water still available there steams out.

If the core melts under low pressure, in about 15 minutes the lower walls of the pressure vessel are heated up to such an extent that the bottom head melts through and the core melt slumps into the reactor cavity. During this process, no reaction forces occur at the anchoring of the pressure vessel.

If the core melts down under high pressure, the failure of the core support structure is very quickly followed by a failure of the reactor pressure vessel already at considerably lower temperatures. The highest thermal stresses occur in the walls of the bottom head. The Study assumes that the entire spherical shell crashes into the reactor cavity. An annular discharge area of several square meters results.

The failure of the reactor pressure vessel is accompanied by a rapid depressurization. During this process, considerable stresses occur which act on the pressure vessel anchoring, the reactor coolant pipes and the surrounding concrete structures (Fig. 7-1).

The Study includes detailed calculations with respect to these stresses, to the load-bearing capacity of the reactor pressure vessel anchoring and to the reactor coolant pipes. Results of these analyses show that the reaction forces resulting from a failure of the pressure vessel can no longer be absorbed by the support lugs of the suspension system at an internal pressure of more than 3 MPa. An upward motion of the pressure vessel is hindered by the interaction between the ring girder fixed to the support lugs and the concrete structures of the inner reactor compartments.

At internal pressures higher than 8 MPa it can no longer be excluded that the containment will also be damaged. However, there is no fear of such a consequential damage to the containment if a failure would occur at another point of the reactor pressure vessel prior to its melt-through. In such a case, the accident sequence might lead to a core meltdown under low pressure (similar to the LP* case) so that the suspension of the reactor pressure vessel would not be endangered if the reactor pressure vessel fails. As far as the early failure of hot structural parts is concerned, confirmed analysis results are not available at present. Thus, the Study does not include any assessments concerning this issue.

For an accident sequence involving a core meltdown under high pressure (HP), the Study estimated an occurrence frequency of approximately $5 \cdot 10^{-7}$/a. As such accidents may lead to serious offsite damages, it is necessary – despite of their low occurrence probability – to further investigate core meltdown processes under high pressure and the resulting loads.

7.4 Hydrogen Combustion

In a core meltdown accident, there are two phases during which larger amounts of hydrogen are generated and get into the containment.

On the one hand, hydrogen is formed when, during the heatup and melting of the fuel rods, steam reacts with the zircaloy cladding tubes of the fuel rods and is reduced to hydrogen (zirconium/steam reaction). Furthermore, large amounts of hydrogen are generated after the reactor pressure vessel has failed and the concrete melts. Water of crystallization evaporates after its release from the concrete. The rising steam passes through the core melt and is reduced to hydrogen as a result of the oxidation of metallic shares in the molten mass and in the concrete. Experiments carried out at the Nuclear Research Center at Karlsruhe concerning the core melt-concrete interaction revealed that more hydrogen is released, in particular during the hot initial phase of the interaction, than had been assumed in earlier analyses [ALS 87a].

Fig. 7-2 shows the total amount of hydrogen released into the containment during a core meltdown accident (LP* case), plotted against time. The first increase is due to the zirconium/steam reaction when melting the fuel elements. During this process, about 50% of the zirconium are oxidyzed, and approximately 600 – 700 kg hydrogen are released into the containment, until the evaporation of the residual water in the reactor pressure vessel begins. The remaining zirconium inventory is converted after the melt-through of the reactor pressure vessel, above all in the initial phase of the core melt-concrete interaction. Thus, a total of nearly 1350 kg hydrogen are released into the containment within just a few hours. The generation of hydrogen during the further penetration of the core melt into the concrete is determined by the oxidation of other metallic components contained in both the melt and the concrete (chromium, iron, etc.).

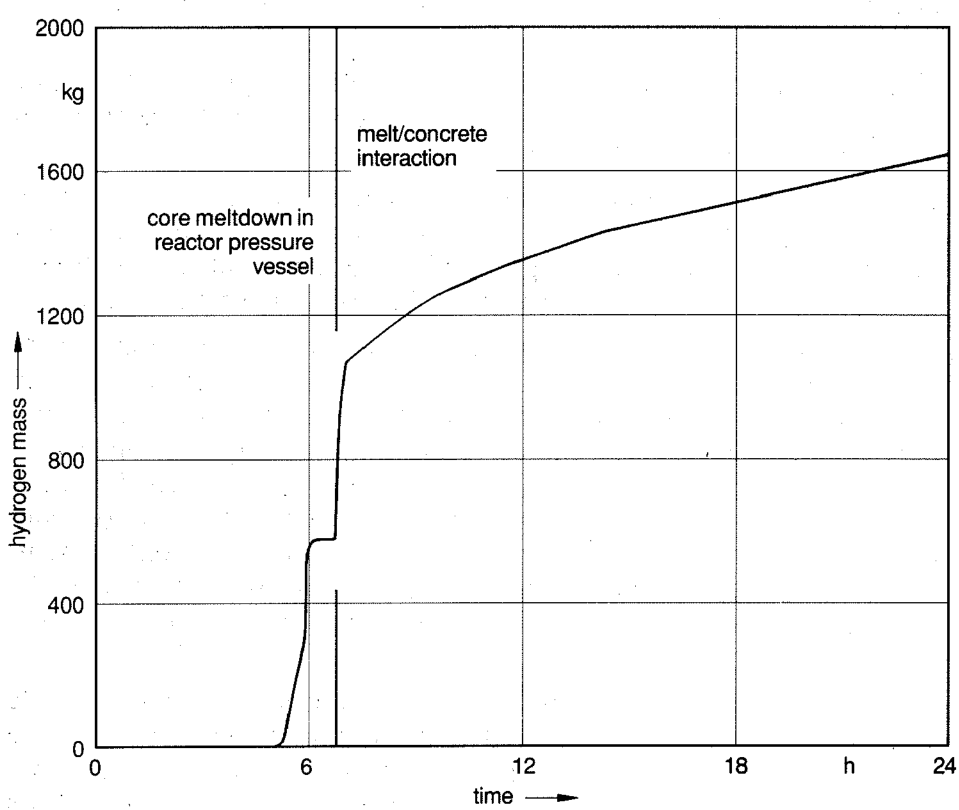


Fig. 7-2:
Amount of hydrogen released into the containment during a core meltdown accident (LP*case).

If a higher accumulation of hydrogen, and thus a combustible mixture of gases, can be generated in the containment, an ignition of the gas mixture leads to a combustion of the hydrogen. The combustion involves an energy input into and a short-term load (pressure peak) acting on the containment.

A higher concentration of hydrogen in the air/steam atmosphere of the containment is avoided if the combustion of hydrogen sets in at an early time. With a sufficient amount of oxygen in the containment, the combustion process may be initiated by existing ignition sources such as electric motors as soon as the ignition limit is reached. So, a hydrogen combustion occurred during the TMI accident had probably been triggered by electric sparks.

The Study investigated the hydrogen distribution in the containment and the loads acting on the containment which may arise from a combustion of hydrogen. The results of these investigations are outlined below.

If an ignition or combustion of hydrogen is effected prior to the failure of the reactor pressure vessel, the resulting loads will not directly interfere with the integrity of the containment.

However, an early ignition of the hydrogen, e.g. prior to the failure of the reactor pressure vessel, cannot be postulated with certainty in view of the steam-containing atmosphere of the containment. The hydrogen may also reach a higher concentration before an ignition occurs.

During the first few hours of release, and in particular immediately after having failed the reactor pressure vessel, the highest hydrogen concentrations will be found in the central and the lower plant compartments. In this process, explosive gas mixtures may develop locally, e.g. in the central and lower steam generator compartments. Potential effects of local detonations, however, are limited by the massive concrete structures in the lower compartment areas of the containment. Therefore, a detonation which would jeopardize the integrity of the containment during this phase of the accident is not considered in the Study.

If, over a protracted period of time, higher concentrations of ignitable mixtures of gases can be generated in the containment atmosphere, the containment is jeopardized in case of occuring a hydrogen combustion. This would apply, for example, if an ignition of the gas mixture occurs not earlier than one or two hours after the reactor pressure vessel has melt through. Within this time, practically the entire zirconium inventory of the cladding tubes has oxidized. This corresponds to an amount of about 1350 kg hydrogen which has been released into the containment by this time. A complete combustion of this hydrogen would lead to pressure peaks reaching the failure pressure of the containment (approximately 0.85 MPa). A later ignition during the longer-term core melt-concrete interaction and the resulting combustion of larger amounts of hydrogen would exceed the failure pressure of the containment.

Countermeasures aiming at a limitation of the hydrogen concentration in the containment and the prevention of a dangerous combustion are being investigated. Igniters, for example, can be installed in vulnerable plant compartments in order to limit the hydrogen content in the containment atmosphere if there are combustible mixtures of gases. With a high portion of steam in the gas mixture, e.g. a share of about 40%, an ignition is unlikely. Then hydrogen can only be removed by metallic foils for catalytic burning. Such foils which are also effective at high steam concentrations and a low hydrogen content are being tested. Further development, however, is needed for the practical application of igniters and catalytic foils as well as for the demonstration of their functional safety. Since technical planning and concept documents had not yet been available when this Study has been completed, the effectiveness of such measure could not be assessed.

7.5 Core Melt-Concrete Interaction and Depressurization of the Containment

The processes during the core melt-concrete interaction as well as the involved pressure loads and thermal stresses acting on the containment have been investigated when studying the long-term containment behavior. These investigations included recent findings obtained from the experiments which have been carried out at the Nuclear Research Center at Karlsruhe and from theoretical studies [ALS 87b].

An accident sequence after a core meltdown at low pressure (LP, LP*) has been investigated. Immediately after the meltthrough of the reactor pressure vessel, the core melt moves mainly downward and penetrates into the concrete foundation. The inner concrete structures at the sides cannot be penetrated by the molten mass before approximately seven to eight hours (Fig. 7-1).

Whether or not the molten mass will be flooded by water from the containment sump cannot be predicted. Should there be a contact with the sump water, it is probable that the surfaces of the molten mass will become incrusted and that a complete flooding of the molten mass is prevented. If no active measures will be taken from outside in order to flood the molten mass, a "dry" interaction between molten mass and concrete can be expected in general.

Even if the molten mass is flooded, the present state of knowledge indicates that further penetration of the molten material in the concrete foundation cannot be stopped as the molten mass is not sufficiently cooled in spite of being entirely covered by water. After about five days the molten mass reaches the bottom edge of the building foundation.

Even if a breakthrough of the molten mass is prevented by the cooling effect of the groundwater, great thermal stresses and mechanical loads acting on the bottom edge of the foundation will lead to cracks and gaps. Fission products may then be leached from the surface crusts of the molten mass-concrete mixture, and get into the groundwater.

At a "dry" molten mass-concrete interaction only a slow and limited pressure buildup will take place in the containment even on a longterm basis. The pressure is mainly determined by the gases released during the destruction of the concrete (steam, hydrogen, CO, CO_2, etc.) The design pressure of the containment (0,57 MPa) would only be reached after about 14 days. If the molten mass is flooded by the sump water, the evaporation of the water leads to a faster pressure buildup. In such a case, the design pressure is reached after about four days.

The Study determined a failure pressure of 0.85 MPa for the failure of the containment due to excessive pressure. As this pressure will be reached only after several days, even if the molten mass gets into contact with sump water, i.e. even if there is a continuous generation of steam, a sufficient amount of time will be available in order to prevent an overpressurization failure of the containment by means of a selected depressurization.

A depressurization of the containment can also mitigate the consequences associated with the meltthrough of the concrete foundation. Thus, the mixture of concrete and molten mass can be relieved from its active forces prior to the meltthrough of the foundation, and the release of fission products into the soil can be mitigated.

Fig. 7-3 shows the pressure time dependence in the containment with depressurization for an LP* accident sequence involving sump water contact. In this particular case, depressurization is effected after about four days, when the pressure in the containment has reached the design pressure. If the depressurization is accompanied by an injection of

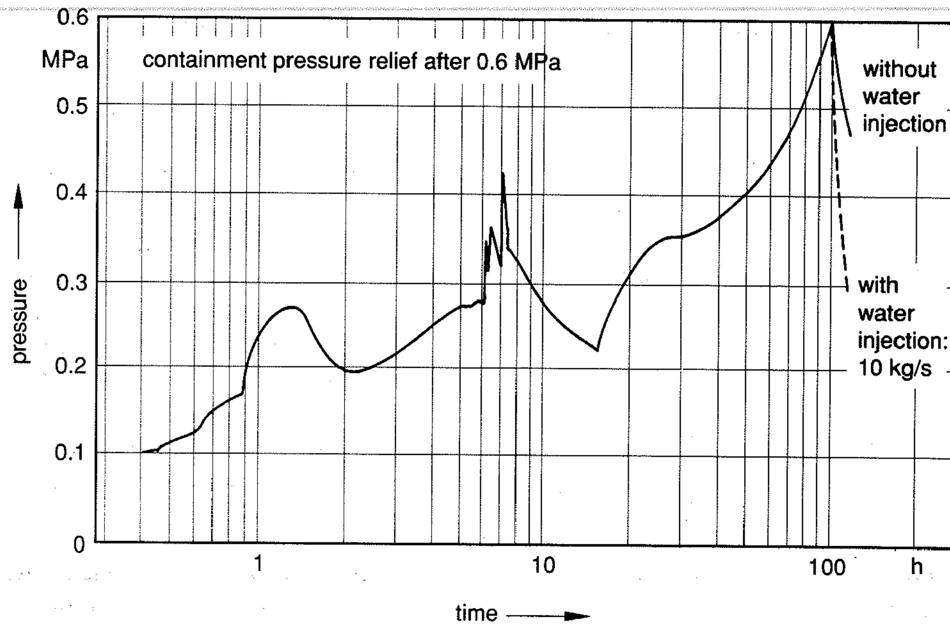


Fig. 7-3:
Pressure time dependence in the containment during a core meltdown accident with sump water-entry and containment venting

water into the containment, an intensified steam generation is avoided and depressurization supported.

It is intended to provide the plant with a depressurization system for the containment. A release of fission products into the environment associated with the depressurization is to be limited by filters. However, this presupposes that the system is prevented from being jeopardized by a combustion of hydrogen.

8. Fisson Product Release

8.1 General

To what an extent radioactive substances will be released into the environment of the plant, as a consequence of a core meltdown accident, essentially depends on how much of the fission products released from the nuclear fuel will be retained in the containment. With the containment remaining tight for a longer period of time, a very great amount of the fission products released from the molten mass can be retained.

Since the completion of Phase A, in the German Core Meltdown Program for Light Water Reactors and at the level of international cooperation, various experiments and theoretical investigations have been carried out with respect to the behavior of the fission products released during a core meltdown accident. Thus, for the release of fission products from the molten mass, the nuclide-specific releases as a function of temperature have been determined in the scope of a test program of the Nuclear Research Center at Karlsruhe [ALB 84]. Moreover, the computer codes describing the behavior of fission products released into the containment, and in particular the decomposition processes in the containment atmosphere have been verified by large-scale technical experiments [SCH 84].

During a core meltdown accident, great amounts of steam, gases and aerosol particles suspended in them are released from core and structural materials into the containment. So, about 1000 kg of dispersed aerosol particles may be in the containment at the beginning of the molten mass-concrete interaction. The majority of these particles, i.e. about 95%, are not radioactive. However, most of the radioactive substances released from the molten mass are bound to aerosol particles.

At the beginning, the concentration of aerosol particles in the humid atmosphere of the containment is very high, but is then very rapidly reduced by various deposition and condensation processes. The aerosol particles are deposited on inner surfaces of the containment or enter the water in the building sump. All in all, the concentration of airborne aerosols decreases by several orders of magnitude within a few days.

The extent, however, to which radioactive substances can be released into the environment during a core meltdown accident decisively depends on the protective function of the containment. If this protective function is not impaired at an early point of time, the containment has an extremely high retention capability. If the containment remains tight over a longer period of time, e.g. over several days, practically all of the fission products released from the molten mass into the containment (with the exception of noble gases) can be retained in the plant. In such a case, the activity release into the environment as a consequence of a core meltdown accident is very low. A large activity release is possible, however, if the containment fails early, if it has larger leaks from the outset or if its retaining function is bypassed right from the beginning.

For core meltdown accidents, a total occurrence probability of approximately $4 \cdot 10^{-6}/a$ has been determined. In this context, both the accident sequences which may lead to an early release of fission products into the environment and the sequences followed by a later release of activity have been investigated.

As a general rule, the activity releases connected with the acccident sequences under review and their occurrence frequencies have to be computed. The investigations concerning core meltdown accidents are still affected by great uncertainties. In particular, it is not possible at present to quantify with a sufficient degree of accuracy the probabilities for the occurrence of the various loads. This applies especially to loads occurring during a core meltdown at high pressure and to such arising from a combustion of hydrogen in the containment. Frequencies of activity releases connected with the individual accident sequences have therefore not been quantified in Phase B.

Nevertheless, it makes sense to compute the releases of fission products for the various accident sequences which have been investigated. The release computations reveal where further research should be done and where technical countermeasures can be used to further improve the retention of fission products in the plant.

In principle, accident sequences connected with very large releases are always conceivable. Irrespective of the safety-related state of a plant, large amounts of the activity inventory enclosed in the plant are always released into the environment. If such accident sequences cannot be ruled out a hundred percent, additional technical countermeasures may not influence the maximum potential damage itself, but can considerably reduce the frequency of a serious damage.

8.2 Computations of Radioactive Releases

- **Results**

In Table 8-1 the activity releases into the environment are compiled as computed for various accident pathways. The cumulative releases related to the core inventory of the respective group of nuclides are quoted.

No retention can be assumed for the noble gases (krypton, xenon).

Table 8-1:
Fission product release from the plant, gauged by core inventory for various accident sequences.

	Kr-Xe	J	Cs	Te	Sr	Ru[1])	La[2])	Ce[3])	Ba
F1-SBV	1E+00	[0,5	bis	0,9]	4E-01	1E-05	2E-02	4E-02	3E-01
F2-PLR	1,0E+00	3,7E-01	3,7E-01	2,3E-01	1,7E-01	2,5E-06	6,4E-03	1,4E-02	1,1E-01
F3a-DE	1,7E-01	1,5E-01	1,5E-01	5,0E-02	6,7E-05	8,8E-08	7,0E-09	--	1,4E-03
F3b-DE	1,7E-01	2,5E-02	2,5E-02	1,5E-02	1,3E-05	1,7E-08	1,3E-09	--	2,7E-04
F4-leak LP*	1,0E+00	7,8E-03	3,5E-04	2,1E-03	1,5E-04	3,6E-07	5,6E-06	1,3E-05	1,3E-04
F5-pressure relief LP*	9,0E-01	2,0E-03	3,3E-07	3,5E-06	2,0E-07	6,4E-10	6,3E-08	2,0E-08	1,7E-07
F6-DF				not analysed					

F1-SBV:	release with large-scale failure of containment
F2-PLR:	release in case of an uncontrolled primary circuit leak in annulus (rupture of residual heat removal line)
F3-DE	release in case of to uncontrolled rupture of steam generator tube w/o (F3a) or with (F3b) refilling of water in defective steam generator
F4-leak LP*	release in case of a small leak (10 cm^2) in containment
F5-pressure relief LP*	release in case of containment venting
F6-DF	release with meltthrough of base plate

1) contains Tc, Rh, Pd, At

2) contains Pr, Nd, Pm, Sm, Eu, Gd, Tb, Dy, Ho, Er, Tm, Yb, Lu, Hf, Ta, W, Re, Os, Ir, Pt, Au, Ac

3) contains Th, Pa, U, Np, Pu, Am, Cm, Bk, Cf, Es, Fm, Md

Thus, they are almost completely released in most of the cases. Very high release rates are possible during accident sequences which lead at an early time to an extensive failure of the containment. They may occur during core meltdown at high pressure or during core meltdown at low pressure with a subsequent combustion of hydrogen which destroys the containment. They are summarized under the heading F1-SBV. No individual analyses have been carried out with respect to the releases quoted here. They only have been estimated. In doing so, it has been assumed that in case a containment failure occurs at least 50% of the volatile nuclides (iodine, cesium or tellurium) are released and that larger amounts of nuclides which are not easily volatilized are released during the molten mass-concrete interaction.

High releases also result for the uncontrolled rupture of a residual heat removal pipe in the annulus (F2-PLR). In this accident, about two-thirds of the fission products are retained if there is no hydrogen combustion in the annulus.

Accident sequences resulting from uncontrolled leaks in steam generator heating tubes (F3a-DE and F3b-DE) lead to considerably lower release rates, in particular if the defective steam generators can be refilled with water prior to the beginning of core meltdown. It is assumed in these cases that the primary circuit pressure has been reduced in time by accident management measures on the primary side in order to avoid a core meltdown at high pressure. Consequently, the major part of the fission products gets into the containment. Only such releases have been taken into consideration which occur prior to the meltthrough of the reactor pressure vessel (after approximately 12 h). Releases during the molten mass-concrete interaction have not been investigated.

Due to the intended backfitting measures, core meltdown accidents connected with large leaks of the containment (e.g. when failing the isolation of the ventilation lines, FK2 in Phase A) need not be considered.

For accident sequences in connection with small leaks of the containment, releases have been calculated starting from a leak of 10 cm^2 (100 times the design leak) [F4 leakage]. During this accident, most of the fission products are retained along the release pathway “containment-annulus-auxiliary building-environment“. A resuspension of deposited fission products during a possible combustion of hydrogen has not been taken into consideration.

If the integrity of the containment is preserved for a long time, the release of fission products during a filtered depressurization (F5 depressurization) is very small. Here, by far the greater part of the fission products is deposited on inner walls of the containment or retained in the sump water. Aerosol particles still airborne in the containment atmosphere at the time of depressurization, are to a large extent absorbed by filters.

Releases during the meltthrough of the foundation has not been investigated in detail. A release is possible if fission products are leached out by groundwater at the lower edge of the foundation. Unless a massive release into the environment has occurred before, engineered countermeasures (e.g. sheet pilings) can be used to limit the release of fission products into the close-range groundwater.

• Comparison with Phase A

The results of the release computations can be compared with those performed in Phase A.[1])

Releases F1 resulting from an early and extensive failure of the containment correspond to those of Release Category FK1 in Phase A. In both cases, the activity release is accompanied by a high release of thermal energy. FK1 of Phase A was a representative collection of accident sequences which lead to an early and extensive failure of the containment. In particular, it has been assumed that a steam explosion in the reactor pressure vessel would also damage the containment. For this accident, Phase A estimated an occurrence probability of approximately $2 \cdot 10^{-6}$/a. In Phase B, the total core meltdown frequency has been determined as $4 \cdot 10^{-6}$/a, i.e. a value that is only slightly higher in the same order of magnitude. If a combustion of hydrogen jeopardizing the integrity of the containment can be prevented by means of engineered countermeasures, the occurrence frequency of accidents involving an early and extensive failure of the containment is lower in Phase B than that of FK1 in Phase A.

Releases F2 are roughly comparable with those of FK2 in Phase A. Although they result from different accident sequences (F2 uncontrolled rupture of a residual heat removal pipe in the annulus; FK2 failure of the building isolation), they both lead to large activity releases near the soil. For the accident sequence of F2, however, a very low occurrence probability ($< 10^{-7}$/a) has been determined which is by about on order of magnitude below the occurrence frequency of FK2 (approximately $6 \cdot 10^{7}$/a) in Phase A.

Accident sequences with respect to an uncontrolled leak in a steam generator heating tube have not been investigated in Phase A. The releases F3a and F3b determined hereto in Phase B, can only conditionally be compared with those of FK3 and/or FK4 in Phase A. They

[1]) GRS 79, Main Volume, p. 167, Table 6-3: Release Categories

occur far later than the activity releases stated in FK3 and FK4 of Phase A with respect to limited leakages of the containment.

The releases with respect to F4 (small leak in the containment) more or less correspond to those of FK4 in Phase A, although they are lower.[1])

The releases during F5 (depressurization of the containment) are comparable with those of FK5 and/or FK6 (failure of the containment caused by overpressure after approximately one day) in Phase A. With the exception of noble gases and elementary iodine, for which no retention in the filters has been assumed, the release terms are considerably lower than in Phase A.

9. Summary

9.1 Discussion of the Results

• Investigations of Systems Engineering Features

In Phase B of the Study far more detailed investigations of systems investigatins engineering features have been performed than in Phase A.

All in all, the frequency of event sequences not coped with by the safety systems is about $3 \cdot 10^{-5}$/a. Hereto, in Fig. 9-1, the proportional contributions of all triggering events to the frequency of uncontrolled event sequences (damage conditions) are plotted as well as the shares of safety system failures included therein. The largest contributions to the frequency of sequences not coped with by safety systems result from operating transients (approximately 50%) and loss-of-coolant accidents via small leaks (approximately 25%). These contributions are mainly due to failures of steam generator feeding and main steam delivery.

Impacts resulting from fire, flooding or external events make a contribution of about 12% to the total frequency of plant states not coped with by systems engineering. The major share results from transients caused by earthquakes.

---

[1]) With the fission product retention in the annulus and the auxiliary building as described in F4 (10 cm^2 leak), Phase B, releases are considerably lower than for FK4 (approximately 5 cm^2 leak) of Phase A in which this retention is not considered.

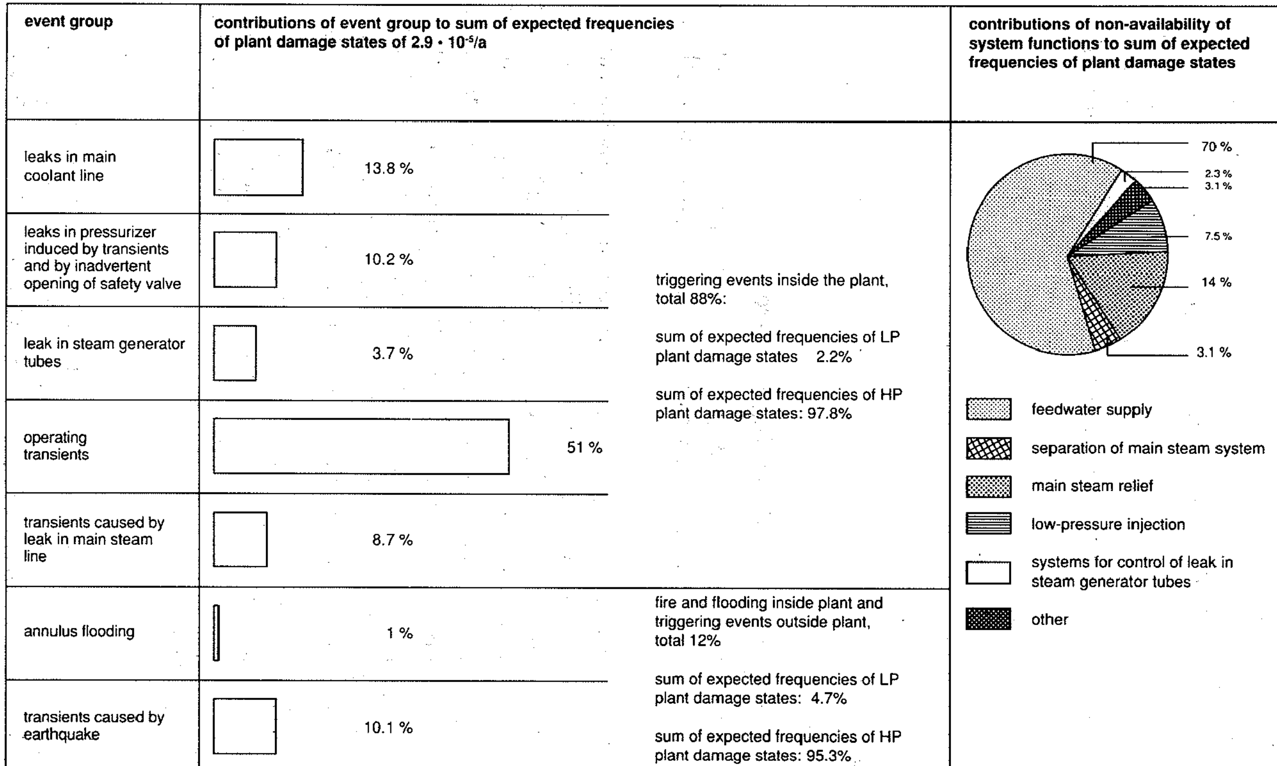


Fig. 9-1:
All triggering events
Contributions to the frequency of accident sequences not coped with by safety systems
(expected frequency of plant damage states)

In Phase A, a total frequency of approximately $9 \cdot 10^{-5}$/a was determined for event sequences not coped with. Inspite of the extended scope of analyses in Phase B more triggering events have been investigated than in Phase A the corresponding value of Phase B, i.e. approximately $3 \cdot 10^{-5}$/a, is lower than in Phase A by about a factor of three. In this context, triggering events already investigated in Phase A account for about 50% of the value determined in Phase B, or a share of $1.5 \cdot 10^{-5}$/a. This more favorable result is mainly due to improvements of systems engineering which have been carried out at the plant following the completion of Phase A. In Phase B, contributions which were leading in Phase A, have been found to be smaller than in Phase A by about one order of magnitude. They include for example contributions to the frequency of an uncontrolled small leak in a reactor coolant pipe and to the frequency of an uncontrolled loss of preferred power.

About the same share of about 50%, or approximately $1.5 \cdot 10^{-5}$/a, results from triggering events additionally investigated in Phase B. Here, important contributions result for uncontrolled accident sequences from pressurizer leaks and inadvertent opening of a safety valve, the failure of the main heat sink and from leaks in the main steam system.

The investigations performed in Phase B of the Study have taken into account all modifications derived from interim results and have already been implemented or will be implemented by the licensee in the near future. These modifications also include supplements to the operating manual concerning measures oriented towards certain aims of protection for the control of accidents.

As is shown in Fig. 9-1, failures of the feedwater supply for the purpose of feeding the steam generators account for about 70% of the occurrence frequencies of event sequences not coped with by safety systems. This dominating share will probably be greatly reduced by the additional emergency system which is intended to be installed in the plant. Moreover, an improved activation of the small safety valves (15% safety valves) in the main steam pipes is scheduled. These measures would further reduce the occurrence frequencies of the accident sequences not coped with by safety systems.

- **Accident Management Measures**

In Phase B, comprehensive plant dynamic analyses have been carried out by which accident sequences could be simulated more precisely and realistic minimum requirements for the effectivenesses of the safety systems have been derived. These investigations have revealed the importance and the risk-mitigating influence of accident management measures. The analyses show that even after a failure of safety systems the plant in many cases still disposes of safety margins. These safety margins can be used for accident management measures.

Almost all the event sequences (resulting from transients and small leaks) which are not coped with by systems engineering lead to a plant condition under high pressure in the reactor coolant circuit. At the beginning, these event sequences involve slow changes in the reactor coolant loop which do not lead to an immediate core meltdown.

In the plant a number of various and flexible possibilities are existing in order to take emergency measures for the prevention or at least the retardation of a core meltdown after the failure of safety systems. In this context, the Study in detail deals with measures to restore the core cooling and the residual heat removal from the reactor after a depressurization of the reactor system and before fuel can start to melt.

For the investigations carried out in the Study, detailed documents were not yet available which would have allowed a detailed assessment of accident management measures. Therefore, only a preliminary assessment of the accident management measures has been possible. With measures to restore the core cooling, performance of which is possible on both the secondary and the primary side, it has been assumed that these measures will be successful in 99 out of 100 cases. For several event sequences involving less favorable plant or time conditions, a lower probability of successful implementation has been set up.

Related to the overall result, it has been estimated that in about 90% of all accident sequences not coped with by systems engineering, the accident management measures investigated can prevent a core meltdown by depressurization and restoration of core cooling (bleed and feed). In particular, and even if measures to restore the core cooling should fail, a core meltdown at high pressure can be prevented by high pressure relief of the reactor coolant circuit before core meltdown sets in.

With these measures, the occurrence of uncontrolled accident sequences calculated to be approximately $3 \cdot 10^{-5}$/a is reduced by about one order of magnitude. Thus, a frequency of approximately $4 \cdot 10^{-6}$/a results for core meltdown at low pressure and a frequency of approximately $5 \cdot 10^{-7}$/a for core meltdown at high pressure.

• Core Meltdown Accidents

Concerning the analysis of core meltdown accidents, results from recent research projects and the investigations performed in the scope of the Study have led to a change in the assessment of a number of several aspects, as compared with earlier evaluations.

Phase A used relatively simple models for the analysis of core meltdown accidents. Analogous to the approach in the US Reactor Safety Study WASH 1400, the Study did not in detail deal with the phenomenological sequences of all possible core meltdown accidents. Thus, only core meltdown at low pressure was dealt with as a representative accident pathway. At that time, phenomena and loads which may occur at core meltdown under high pressure were not investigated.

Substitutionally for accidents involving an early and extensive failure of the containment, Phase A postulated a steam explosion in the reactor pressure vessel which destroys the reactor pressure vessel and, at the same time, damages the containment. The evaluations of experiments and theoretical investigations of steam explosions reveal that a violent steam explosion which may destroy the containment cannot occur or is at least extremely improbable. It therefore is excluded as a risk-relevant accident pathway in Phase B.

Nevertheless, in accordance with the present state of knowledge and with the investigations carried out in Phase B, accident sequences are possible which may jeopardize the integrity of the containment at an early time. They can occur during core meltdown at high pressure or may be caused by a combustion of hydrogen in the containment.

Both accident scenarios require further investigations. With respect to accident sequences involving a core meltdown at high pressure, it has to be clarified, e.g. whether a failure at any other point of the reactor coolant circuit may occur before the reactor pressure vessel fails.

In accordance with the state of knowledge at that time, it was assumed in Phase A that the hydrogen generated during a core meltdown accident will burn continuously. The investigations in Phase B, however, show that higher concentrations of hydrogen may be generated in the containment which may jeopardize the containment if they are ignited. Engineered countermeasures (igniters, catalytic foils) are being investigated which may limit the hydrogen content in the containment and prevent a dangerous combustion. However, further development work is required prior to the large-scale application of such measures.

If a hydrogen concentration jeopardizing the containment in the case of combustion can be ruled out, the occurrence frequency of an early and extensive containment failure is lower in Phase B than it was in Phase A.

Because of backfitting measures, accident sequences involving a large leak in the containment (e.g. in the case of failing a ventilation pipe isolation) do no longer make a risk-relevant contribution. This applies also to accident sequences which are initiated by an uncontrolled leak in a connecting pipe of the reactor coolant circuit in the annulus, since corresponding backfitting measures are being taken.

If the integrity of the containment remains intact for a longer period of time, a depressurization prevents overpressure failure of the containment. Most of the fission products released from the molten mass are deposited in the containment and/or retained by filters.

The fission product release involved in the meltthrough of the building foundation has not been determined. The effects, however, are mitigated by means of containment venting. Moreover, engineered countermeasures are possible, such as the application of sheet pillings, in order to limit the release to the close area.

All in all, the assessment of the loads acting on the containment after core meltdown accidents is affected by considerable uncertainties.

9.2 Limitations of the Study

For the investigations a number of limitations result which have to be taken into consideration in an assessment of the results.

A risk study cannot investigate in detail all the event sequences which are conceivable. In principle, the completeness of a risk study cannot be demonstrated. It may only be verified on the basis of the systematic approach of an analysis, evaluations of operating experience and the current state of knowledge in safety research.

As compared with Phase A, Phase B includes the detailed analysis of a number of additional triggering events. In doing so, the scope of investigations has been considerably extended as compared with Phase A. On the other hand, however, various triggering events which are not expected to make any noteworthy risk contributions have not been investigated. For example, reactivity accidents, accidents during startup and shutdown of the reactor as well as such occurring during the inspection have not been analyzed in detail.

The occurrence frequencies of "more frequent" operating disturbances and the reliability data of important components have been mainly determined on the basis of plant-specific operating experience. Furthermore results of systems engineering analyses may to a large extent also be verified today on the basis of operating experience, e.g. the evaluations of in-service inspections. On the other hand, however, a risk analysis also has to consider rare events for which little or no operating experience is available. An example hereto is the occurrence frequency of large pipe ruptures. In this case, theoretical estimates are needed wich are affected by great uncertainties. The same applies to the evaluation of common cause failures and of human failure, results of which are also affected by great uncertainties.

The accident management measures taken into consideration in the Study are only assessed on a preliminary basis.

To a large extent, the investigations of core meltdown accidents are based on the modelling of phenomena which still requires further experimental verification. Therefore, the analysis of loads occurring during a core meltdown accident is still affected by considerable uncertainties. Thus, it is not possible at present to quantify the risk involved in core meltdown accidents.

It has not been the aim of this Study to investigate all the possible influences which make a contribution to the risk of nuclear power plants.

So the Study only investigated the possible risk contributions due to accidents, but not the risk involved in the continuous operation of nuclear power plants. Risk contributions made by possible enemy action and sabotage have not been dealt with. They would not lead, however, to accident sequences which in principle are different from those considered in this Study.

9.3 Conclusions

The investigations show that, in many cases, results depend on details of systems engineering and are of a plant-specific nature. This applies in particular to accident event sequence analyses and reliability investigations. Therefore, the results determined for Biblis B cannot right away be applied to other nuclear power plants equipped with a pressurized water reactor.

However, the investigations and results of the Study give concrete hints how to proceed when assessing other plants. The results of Phase A, for example, led to systems engineering improvements not only at the reference plant. The results have also been considered in the safety design of recent plants, e.g. the convoy plants. Examples to be quoted in this context include the possibility of high-pressure safety injection by sump recirculation and the accident-resistant design of the feedwater control system.

Correspondingly, it can also be checked to what extent the results determined in Phase B and the safety improvements identified in this context are of importance to other plants. Because of the continuous progress in the development of safety engineering, it is expected that, at more recent plants, the occurrence frequency of a core meltdown will be lower than that determined by the investigations performed in Phase B.

In all, the work carried out and the results obtained in Phase B confirm that probabilistic safety analyses can be used to verify and to further improve the safety design of a plant. Thus, probabilistic safety analyses greatly contribute to the further development of the plant concept.

In order to improve the certainty of the results obtained from plant engineering investigations, a systematic evaluation of operating experience gathered at nuclear power plants is necessary. In this way, the database for independent failures, common cause failures and for the assessment of measures taken by the operating personnel can be improved.

During the work carried out for Phase B, the importance of accident management measures has been recognized. Even if design limits are exceeded, there are still possibilities for an application of accident management measures to prevent a core meltdown or to mitigate effectively the consequences of a core meltdown accident. Thus, analyses concerning accident management measures belong to the major aspects of Phase B of the Study.

Detailed analyses have been carried out concerning measures to restore core cooling after a depressurization of the reactor cooling circuit and before core meltdown can set in. Although these measures cannot yet be finally evaluated, the analyses show that they considerably reduce the risk involved in accidents at nuclear power plants. It therefore is important that further investigations are made to probe the safety potential of accident management measures and to make use of this potential in the further development of the safety concept. In order to reduce the uncertainties in the evaluation of accident management measures, simulation models should be provided by means of which instructions can be prepared how to proceeed in unusual situations.

Risk studies are used to evaluate in a greater context the findings obtained from individual research projects. In doing so, gaps in knowledge are detected which require further research and development. Therefore, risk studies may be used to set priorities for the planning and implementation of research projects.

In the Study, corresponding suggestions result from the investigations of core meltdown accidents. Further investigations are necessary particularly for core meltdown at high pressure, for the behavior of hydrogen and for the meltthrough of the reactor foundation. In this context, further development has to include engineering measures by means of which possible injurious consequences of accidents can be effectively limited.

High release rates result wherever accident event sequences under investigation are followed up until they have developed into extreme accident scenarios. The Study determined very low occurrence probabilities for such accident scenarios. In this context, phenomena and loads occur which can often no longer be analyzed in detail and the probabilistic evaluation of which is very difficult.

Irrespective of the efforts made in safety engineering certain accident scenarios are conceivable in which fission product barriers are not effective any longer. Although additional safety precautions can be taken to reduce the occurrence frequency of severe damages, the danger potential remains the same and the extent of the damage as such cannot be decisively influenced. Accident sequences outside the plant which involve severe and serious consequences were already estimated in Phase A. For this reason, computations of accident consequences have not been performed again in Phase B.

The results obtained in the Study and the evaluations made in this context refer to the present state of knowledge. Along with the experience which has been gained in the course of the work performed for the Study, both the fields of major emphasis and the objectives of the Study have shifted to plant engineering analyses. In doing so, both a number of backfitting measures concerning systems engineering and of research projects have been suggested which can further improve the safety of the plant and can deepen its safety assessment. It is considered meaningful and necessary to proceed with a continuous evaluation in probabilistic safety analyses of new findings from operation and research in order to determine whether or not safety improvements and a further development of the safety concept are necessary and possible.

Literature

/ALB 84/ Albrecht, H., und H. Wild:
Review of the Main Results of the SASCHA Program on Fission Product Release under Core Melting Conditions
ANS Meeting „Fission Product Behavior and Source Term Research", Snowbird, 15.-19. Juli 1984

/ALS 87a/ Alsmeyer, H.:
BETA-Experiments in Verification of the WECHSL-Code: Experimental Results on the Melt Concrete Interaction
Nuclear Engineering and Design, Vol. 103, S. 115-125, 1987

/ALS 87b/ Alsmeyer, H., u.a.:
Modellentwicklung zur analytischen Beschreibung von Kernschmelzunfällen
PNS-Jahresbericht 1987, KFK 4100, S. 4300-14 bis 32

/GRS 79/ Gesellschaft für Reaktorsicherheit (GRS) mbH:
Deutsche Risikostudie Kernkraftwerke
Eine Untersuchung zu dem durch Störfälle in Kernkraftwerken verursachten Risiko
Hrsg.: Der Bundesminister für Forschung und Technologie
Verlag TÜV Rheinland, Köln, 1979

/GRS 89/ Gesellschaft für Reaktorsicherheit (GRS) mbH:
Deutsche Risikostudie Kernkraftwerke, Phase B
Druck in Vorbereitung

/NUR 87/ U.S. Nuclear Regulatory Commission:
Reactor Risk Reference Document, NUREG 1150, Draft for Comment, Februar 1987

/SCH 84/ Schöck, W., u.a.:
The DEMONA Project, Objectives, Results and Significance for LWR Safety
5th International Meeting on Thermal Reactor Safety
Karlsruhe, 9.-13. September 1984

/SWA 83/ Swain, A.D., und H.E. Guttmann:
Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application
NUREG/CR-1278, August 1983

/WAS 75/ U.S. Nuclear Regulatory Commission:
Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants
WASH 1400 (NUREG 75/014), Oktober 1975

Annex

A.1 Participated Firms and Institutions

After the completion of Phase A, the Federal Minister for Research and Technology (BMFT) requested a number of institutions to continue the work on the German Risk Study Nuclear Power Plants in a subsequent Phase B. Research projects performed for this purpose aimed above all at further deepening individual subjects and at preparing recent knowledges of the German and international reactor safety research for use in risk analyses. The work for this research project has been finished at the end of 1984.

In this work the following firms and institutions have been involved:

Battelle-Institut e.V.
Frankfurt

Beratungs-Büro für Angewandte Physik
Gechingen

Brenk Systemplanung
Ingenieurbüro für wissenschaftlich-technische Beratung
Aachen

Babcock-Brown, Boveri Reaktor GmbH (BBR)
Mannheim

Eidgenössisches Institut für Reaktorforschung (EIR)
Würenlingen/Schweiz

Gesellschaft für Reaktorsicherheit (GRS) mbH
Köln

Gesellschaft für Strahlen- und Umweltforschung mbH (GSF)
Neuherberg

GUW Gesellschaft für Umweltüberwachung mbH
Aldenhoven

Institut für angewandte Ökologie
Freiburg

Institut für Kernenergetik und Energiesysteme (IKE)
Universität Stuttgart
Stuttgart

Kernforschungsanlage Jülich GmbH (KFA)
Institut für Nukleare Sicherheitsforschung
Jülich

Kernforschungszentrum Karlsruhe GmbH (KfK)
Institut für Neutronenphysik und Reaktortechnik (INR)
Projekt Nukleare Sicherheit (PNS)
Karlsruhe

NIS Ingenieur-Gesellschaft mbH
Hanau

Rheinisch-Westfälisches Elektrizitätswerk AG (RWE)
Essen

Rheinisch-Westfälischer Technischer Überwachungs-Verein e.V.
Essen

Siemens AG, UB KWU
Erlangen

Staatliche Materialprüfungsanstalt (MPA)
Universität Stuttgart
Stuttgart

Technischer Überwachungs-Verein Rheinland e.V.
Institut für Unfallforschung und Ergonomie
Köln

Dr.-Ing. Horst Wölfel
Beratende Ingenieure
Höchberg

Zerna, Schnellenbach und Partner
Gemeinschaft Beratender Ingenieure GmbH
Bochum

In 1985 the Federal Minister for Research and Technology appointed the Gesellschaft für Reaktorsicherheit (GRS) mbH to carry on and to finalize work on Phase B of the German Risk Study Nuclear Power Plants, taking into account the results of individual investigations. In the scope of this project GRS awarded subcontracts for the performance of certain subtasks to the following institutions:

Technischer Überwachungs-Verein Norddeutschland e.V.
Hamburg

König und Heunisch
Beratende Ingenieure
Frankfurt

Staatliche Materialprüfungsanstalt (MPA)
Universität Stuttgart
Stuttgart

Institut für Kernenergetik und Energiesysteme (IKE)
Universität Stuttgart
Stuttgart

Kernforschungszentrum Karlsruhe GmbH (KfK) [1])
Projekt Nukleare Sicherheit (PNS)
Karlsruhe

A.2 Lectures and Publications

In the course of performing the Study, reports on the respective state of investigations and progress reports on available interim results relating Phase B were presented at a number of specialists' meetings as well as in several publications. The subsequent list contains a compilation of papers and publications on this work of the past three years.

Lectures given at the Annual Meeting Nuclear Technology '86 of the Kerntechnische Gesellschaft e.V. (KtG) and the Deutsches Atomforum e.V. (DAtF), Aachen, April 8-10, 1986

Birkhofer, A.:
Was leisten Risikostudien?
(atomwirtschaft/atomtechnik, Heft 8/9, 1986, S. 440)

Further lectures given at this meeting in the specialists' session "Results of Phase B of the German Risk Study Nuclear Power Plants"
(published by Deutsches Atomforum, Bonn)

Rininsland, H., A. Fiege und E.F. Hicken:
Stand der Untersuchungen zu schweren Kernschäden (Phänomenologie des Brennstab- und Kernverhaltens im Vorfeld des Kernschmelzens)

Hosemann, J.P., und K. Hassmann:
Methoden zur Quelltermbestimmung bei Kernschmelzunfällen und experimentelle Absicherung

[1]) Mitarbeit im Rahmen des projekteigenen Arbeitsprogramms

Hörtner, H., E.J. Kersting und B.M. Pütter:
Systemtechnische und Ereignisablauf-Analysen

Friederichs, H.G., F.W. Heuser und J. Rohde:
Unfallarten und Freisetzungskategorien

Ehrhardt, J., und H.B. Paretzke:
Modellierung und Abschätzung von Unfallfolgen

Lectures taken from the final colloquium of the Project Nuclear Safety, Kernforschungszentrum Karlsruhe, June, 10-11, 1986
(KFK 4170, August 1986)

Alsmeyer, H.:
BETA-Experimente zur Verifizierung des WECHSL-Codes, Experimentelle Ergebnisse zur Schmelze-Beton-Wechselwirkung

Reimann, M.:
Verifizierung des WECHSL-Codes zur Schmelze-Beton-Wechselwirkung und Anwendung auf den Kernschmelzunfall

Ehrhardt, J., und H.J. Panitz:
Schwerpunkte der Weiterentwicklung des Unfallfolgenmodells UFOMOD und erste Analysen zum Reaktorunfall von Tschernobyl

Lectures given at the 10th GRS-Specialists' Meeting, Cologne, November 12-13, 1986
(GRS-64, März 1987)

Heuser, F.W.:
Risikountersuchungen zu Unfällen in Kernkraftwerken, (siehe auch atomwirtschaft/atomtechnik, Heft 2, 1987, S. 79)

Friederichs, H.G., und E. Schrödl:
Neue Erkenntnisse zur Spaltproduktfreisetzung aus dem Kern und Reaktorgebäude bei Unfällen

Hörtner, H.:
Zuverlässigkeitsuntersuchungen für Sicherheitssysteme und ihr Vergleich mit Auswertungen von Betriebserfahrungen

Liemersdorf, H.:
Beurteilung der Brandgefahr in kerntechnischen Anlagen

Lectures given at the Annual Meeting Nuclear Technology 1987 of the Kerntechnische Gesellschaft e.V. (KTG) and Deutsches Atomforum e.V. (DAtF), Karlsruhe, June 2-4, 1987

Birkhofer, A.:
Sicherheit deutscher Kernkraftwerke
(atomwirtschaft/atomtechnik, Heft 10, 1987, S. 474)

Further lectures of this meeting given at the specialists' session "Safety and Control of Accidents in PWR- and BWR-Nuclear Power Plants" (published by Inforum, Bonn, December 1987

Heuser, F. W., H. Hörtner und E. Kersting:
Risikountersuchungen zur Sicherheitsbeurteilung von Kernkraftwerken

Hennies, H. H., und B. Kuczera:
Stand der internationalen Reaktorsicherheitsforschung

Further lectures/publications:

Birkhofer, A.:
Technische Risikoanalysen: Ein Beitrag zur Technologiebewertung
In: Jungermann, Pfaffenberger, Schäfer u.a.:
Die Analyse der Sozialverträglichkeit für Technologiepolitik. Perspektiven und Interpretationen
High Tech, München, 1986, S. 135

Bracht, K.F., und E.J. Kersting:
Effectiveness of Operational Actions to Manage Severe Accidents Resulting from Station Blackout
IAEA-Seminar on Operating Procedures for Abnormal Events, München, 23.-27. Juni 1986

Heuser, F.W., A. Höfler und H. Schulz:
Analysis of Severe Accidents and Estimates of the Ultimate Loading Capacity of the Steel Containment
Proceedings of the Third Workshop on Containment Integrity, NUREG/CP-0076, August 1986

Chakraborty, A.K., E.J. Kersting u.a.:
An Alternate Possibility to Remove Hydrogen from the Containment Atmosphere during Severe Accidents
ANS/ENS Topical Meeting on Operability of Nuclear Power Systems in Normal and Adverse Environment
Albuquerque, 29. September - 3. Oktober 1988

Beliczey, S., und H. Schulz:
Nutzung bruchmechanischer Methoden und Betriebserfahrung bei der Bestimmung von Eintrittshäufigkeiten für Lecks in Rohrleitungen von Druckwasserreaktoren
12. MPA-Seminar, Stuttgart, Oktober 1986

Birkhofer, A., und K. Köberlein:
Sicherheitsrelevante technologische Trends und ihr Einfluß auf den Bedarf an Risikoabsicherung
In: Gesellschaft und Unsicherheit
Hrsg.: Bayr. Rückversicherung AG, Verlag Versicherungswirtschaft, Karlsruhe, 1987, S. 157

Hörtner, H., und J. von Linden:
German Risk Study, Influences of Data Base, Minimal Requirements and System Changes
9th International Conference of Structural Mechanics in Reactor Technology, Lausanne, August 1987

Kersting, E.J.:
Untersuchungen über Eingriffsmöglichkeiten bei Störfällen mit Ausfall von Sicherheitsfunktionen
11. GRS-Fachgespräch, München, 29.-30. Oktober 1987
(GRS-68, März 1988)

Hörtner, H.:
German Risk Study, Phase B, Results of the Event Tree and Fault Tree Analyses
Proceedings of the International Conference Probabilistic Safety Assessment and Risk Management PSA '87, Zürich, Vol. II, S. 419, Verlag TÜV Rheinland, Köln, 1987

Gruner, P., F.W. Heuser und J. Rohde:
German Risk Study, Phase B, Results on Severe Accident Analysis
International Conference Probabilistic Safety Assessment and Risk Management PSA '87, Zürich, August 1987

Birkhofer, A., und F.W. Heuser:
Probabilistische Sicherheitsanalysen und Risikountersuchungen in der Bundesrepublik Deutschland
Société Francaise d'Energie Nucléaire SFEN
Section Technique „Sûreté Protection de l'Environnement"
SFEN et KTG, Paris, 20. Oktober 1987

Birkhofer, A., und A. Jahns:
Severe Accidents: Analysis, Strategies and Accident Management in the FRG
International Symposium on Severe Accidents in Nuclear Power Plants, Sorrento, Italien, 21.-25. März 1988, Proceeding Series STI/PUB/782

Kersting, E.J., und J. Rohde:
Analysis of Selected Accident Management Measures for a German PWR
International Symposium on Severe Accidents in Nuclear Power Plants, Sorrento, Italien, 21.-25. März 1988, Proceeding Series STI/PUB/782

Birkhofer, A.:
Die Behandlung von Störfällen im Rahmen der Risikostudie
2. Kolloquium der Arbeitsgruppe Umweltstandards: Fakten und Bewertungsprobleme am Beispiel des Strahlenrisikos, Akademie der Wissenschaften, Berlin, 15. April 1988

Birkhofer, A.:
Applications of Safety Research and PSA to Nuclear Plant Design and Operations
EPRI Nuclear Power Division Advisory Committee Meeting, Philadelphia, 20. Mai 1988

Herbold, G., E.J. Kersting und W. Korbach:
Analysis of Secondary Side Oriented Accident Management Measures for a PWR of KWU-Design
1988 IEEE Fourth Conference on Human Factors and Power Plants, Monterey, California, 5.-9. Juni 1988

Kersting, E.J.:
Accident Management Measures
Kerntechnik, Vol. 53/1, Carl Hanser Verlag, München, Oktober 1988

Heuser, F.W.:
Main Results of the German Risk Study, Phase B
NUCSAFE 88, Avignon, Oktober 1988
Proceedings of the International ENS/ANS Conference on Thermal Reactor Safety, Vol. 5, S. 1925

Heuser, F.W., H. Hörtner und E.J. Kersting:
Ereignisabläufe mit anlageninternem Notfallschutz in der Risikostudie
12. GRS-Fachgespräch, Köln, 3.-4. November 1988
(GRS-69, Mai 1989)

Birkhofer, A.:
Anlageninterner Notfallschutz
Achtes Deutsches Atomrechtssymposium, München, 1.-3. März 1989

Birkhofer, A.:
Severe Accident Management
International Topical Meeting on Probability, Reliability, and Safety Assessment PSA '89, Pittsburgh, USA, April 1989

Heuser, F.W.:
Basic Aspects and Results of the German Risk Study, Phase B
Proceedings of the International Topical Meeting on Probability, Reliability and Safety Assessment PSA '89, Pittsburgh, USA, April 1989, Addendum, p. 20

Gesellschaft für Reaktorsicherheit (GRS) mbH

Schwertnergasse 1
5000 Köln 1

Forschungsgelände
8046 Garching

ISBN 3-923875-24-X