Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH

Safety Analysis for Boiling Water Reactors

A Summary

GRS - 98

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) mbH

Safety Analysis for Boiling Water Reactors

A Summary

E. Kersting
J. von Linden
D. Müller-Ecker
W. Werner

Translation by F. Janowski

July 1993

GRS - 98
ISBN 3-923875-48-7

Note

This report is the translation of GRS-95 "Sicherheitsanalyse für Siedewasserreaktoren - Zusammenfassende Darstellung". Recent analysis results - concerning the chapters on accident management, fire and earthquake - that were not included in the German text have been added to this translation. In cases of doubt, GRS-102 (main volume) is the factually correct version.

Keywords
Safety analysis, PSA, boiling water reactor, accidents, event-sequence analysis, systems analysis, fault-tree analysis, reliability data, accident management

Abstract

After completing the German Risk Study for pressurised water reactors, the Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) has now conducted for the first time a probabilistic safety analysis for boiling water reactors (BWR) on behalf of the Federal Minister for Research and Technology (BMFT).

Reactor safety is constantly developed in line with research findings and operating experience. Thus reactor safety is a dynamic process in which safety analyses play an important role. Probabilistic safety analyses determine the frequency of certain events (e.g. leaks in pipes) and the failure probabilities of the safety systems needed to control such events. The failure of safety systems initially leads to a hazard to the cooling of the reactor core. When such hazard states occur, there are accident-management measures which can still be carried out in order to prevent core melt.

The particular aim of this analysis is to examine and evaluate the balance of the safety-related technology, to suggest safety-related improvements, and to show the possibilities of accident-management measures at severe accidents.

The analysis investigates representative safety-relevant events which can lead to damage to the reactor core. The analyses show that there is an expected frequency of approx. $5 \cdot 10^{-5}$/a for the event sequences that cannot be controlled by operational and safety systems (hazard states); this means that there is a probability rate of 1 to 20 000 per plant and year. In the majority of these cases there is relatively much time (more than three hours) available to carry out accident-management measures, which means that there are favourable prospects for their success. Within the framework of this phase of the investigation, however, such measures have not been conclusively assessed.

The calculated frequency does not take into account an additional safety system which is presently being installed: the so-called additional residual-heat-removal and injection system (ARHR-system) with additional shutdown line. At consideration of this additional safety sytem the estimated frequency of uncontrolled event sequences is reduced by a factor of 10 to approximately 1 to 200 000 per plant and year.

Recommendations for a considerable improvement of plant technology and accident-control procedures were already made during the course of the analysis. They have

by now been implemented to a large extent and have led to an increase in plant safety. An overall high level of safety is achieved through the system changes that have already been implemented and those intended to be implemented in the near future.

The study also yields concrete information for the evaluation of other boiling water reactors. Additionally, the analysis identifies unresolved issues which make further research and development work necessary.

In general, the probabilistic safety analysis with its systematic procedure has proved to be a valuable tool for safety evaluations and an effective means for the identification of possible improvements. It presents an example of practice-orientated research with great benefits that can be realised in the short term.

Contents

1 Objectives, Scope and Methodology of the Safety Analysis

The investigations for the BWR safety analysis were performed on behalf of the Federal Minister for Research and Technology and carried out by GRS. Sub-contracts for parts of the work were given to the Technischer Überwachungs-Verein Bayern e.V., Munich, and to König and Heunisch, Consulting Engineers, Frankfurt/Main.

1.1 Objectives of the Investigations

Based on the knowledge gained from safety research and operating experience, the BWR safety analysis has the following objectives:

- to determine the relative significance of event sequences and safety functions
- to examine the balance of the safety-related design
- to suggest and evaluate safety-related improvements
- to demonstrate the potential of accident-management measures.

1.2 Scope of the Investigations

This safety analysis investigates selected safety-relevant events which can lead to core damage.

The investigations concentrate on the systems necessary for the control of the selected plant-internal and external events. All operational and safety systems as well as the measures provided for in the operating manual are included in the evaluation.

The analysis takes into account the changes to the systems technology and to the operating manual that have already been realised by the operator or which will be implemented in the near future. Further modifications, the additional residual-heat-removal and injection system and the additional shutdown line, are assessed separately. The analyses comprise the determination of event sequences that are not controlled by operational and safety systems (hazard states) and of their frequency. Safety analyses of this kind determine the frequency of events (e.g. leaks in pipes) and the failure probability of the safety systems necessary for controlling

them. The failure of such safety systems initially leads to a hazard to the cooling of the reactor core. At that stage, accident-management measures can be carried out in order to control such hazard states or to prevent damage states (e.g. core damage). The safety of the plant is evaluated only up to the level of hazard states. Figure 1-1 shows the hierarchy of hazard states and damage states.

The study shows up the potential of accident-management measures for the control of hazard states. Using existing studies for other plants, it presents an initial estimation for the probabilities of the success of such measures; consequently, no frequencies of damage states (e.g. core melt) are determined in this case.

Results of scoping analyses on incidents outside power operation are discussed.

1.3 Methodology

1.3.1 Investigation Procedure

The safety analysis comprises the following steps to investigate the relevant event sequences:

- identification of initiating events and determination of the expected frequencies
- determination of the event sequences not controlled by the operational and safety systems (hazard states) and their frequencies
- demonstration of the potential of accident-management measures for the control of hazard states, i.e. for the prevention of damage states (e.g. core melt).

1.3.2 Analysis Methods

- Initiating Events

The selection and grouping of initiating events was made with regard to

- whether the event was observed in the reference plant or in other BWR plants, or
- the similarity of the responses of to the event, and of the relevant attending phenomena, or
- whether other studies have recognised the event as an important one.

For the determination of the expected frequencies of initiating events the study uses

- plant-specific information for events for which sufficient data is available from the plant's operating experience (e.g. operational transients);
  for the loss of preferred power - which has not occurred in the reference plant - zero-event statistics are employed
- plant-specific and additional information from other nuclear power plants for events where plant-specific operating experience alone is insufficient (e.g. small leaks up to 10 cm^2)
- the methodology of the German Risk Study Phase B (DRS-B) for small (from 10 cm^2), medium-size and large leaks in pipes
- plant-specific and additional information from other nuclear power plants for events where plant-specific operating experience alone is insufficient, and model scenarios (e.g. ATWS, flooding, fire).

• Analyses of Event Sequences

An initiating event can be controlled by individual functions or by a combination of functions of various safety systems (system functions). Thermodynamic analyses determine which combinations of system functions can achieve this objective. In this respect, the study determines in particular which of the redundant system trains of the individual safety systems are necessary (minimum success criteria) in order to fulfil a certain safety function. If the minimum success criteria are not fulfilled, the event sequence leads to a hazard state. Hazard states are described by characteristic features (plant parameters and the time-span to the onset of a hazard state).

Event-sequence diagrammes systematically outline the possibilities with which initiating events can be controlled or how they can lead to a hazard state. For this

purpose event paths are drawn up, starting from the initiating event and branching off into two paths at each required system function: one path is associated with the availability of the system function, the other one with its unavailability. This results in a large number of paths, leading to either controlled states or hazard states.

In the event-sequence diagramme, probabilities are associated with each branch point. They correspond to the availability or unavailability of the respective system function. The probabilities are conditional on the sequence and are determined by reliability (fault-tree) analyses.

The frequency for each individual path leading from the initiating event to a hazard state is the product of the initiator frequencies and of its branch probabilities. The frequency of a particular hazard state is made up by the sum of frequencies of the individual paths that lead to the same hazard state.

- Systems Analyses

In order to be able to determine probabilities for the branch points in the event-sequence diagramme, the unavailabilities of the system functions have to be qualified. Due to the high reliability of the systems in nuclear power plants, direct observations of system failure are rarely available. On the other hand, data on the failure of components that exist in large numbers in the various systems is available from operating experience. For this reason, the failure of system functions is deduced from the failure of its components. In this context, human errors are treated like component failures.

For the determination of the failure probabilities of system functions, the fault-tree method is used. Given an undesired event (e.g. failure of cooling system), it systematically searches for all possible causes of failure that can lead to the event. In general, there is a large number of combinations of failures of various components or partial systems. Through graphic display, the fault-tree method enables the assessment even of complex systems. It also accounts for subsequent consequential failures, human errors and common-cause failures.

For carrying out the analysis, an overall fault tree is drawn up for each initiating event and each hazard state (top event). The numerical evaluation of the fault trees yields

the mean conditional unavailabilities of the systems needed to prevent a hazard state, given an initiating event.

The determined numerical values are point values obtained from the expected values of the initiating events and from the reliability data of the components. For the assessment of the balance of the safety-related design, which is the main objective of this study, it makes sense to use point values since the focus is on the relations between the determined values. The comparison with point values from other studies must be made with caution because no uncertainty analysis was performed and thus no definite statement can be made on the position of the point values relative to the commonly used distribution measures like median and mean.

- Uncertainty of Data

During the operation of the plant, initiating events and component failures are monitored, and expected frequencies of initiating events as well as reliability data of the components (failure rates, unavailabilities) are deduced. Uncertainties are associated with these values. Distinction is made between the following uncertainties:

- statistical uncertainties due to the limited number of observations (database)
- uncertainties due to varying influences (different components and different conditions of operational use)
- model uncertainties, where models were used for estimations in the case of an insufficient database.

The uncertainties are expressed in terms of probability distributions, describing the possible variation of the data. If the thus quantified uncertainties of the expected frequencies of initiating events and of the reliability data of components as well as the uncertainties associated with the physical modelling were propagated through the calculation steps for the determination of the unavailabilities of system functions, then this would result in (subjective) probability distributions for the unavailabilities of system functions.

The present study does not, however, carry out an uncertainty analysis of this kind as until now only selected events have been investigated; not all issues that may influence the results and their uncertainties have been finally assessed. It is therefore

planned to carry out a comprehensive uncertainty analysis in Phase II of the study, which is to bound the relevant phenomenological uncertainties. For the determination of the unavailabilities of systems, the present study uses the mean values of the distribution functions for failure rates and failure probabilities of the components.

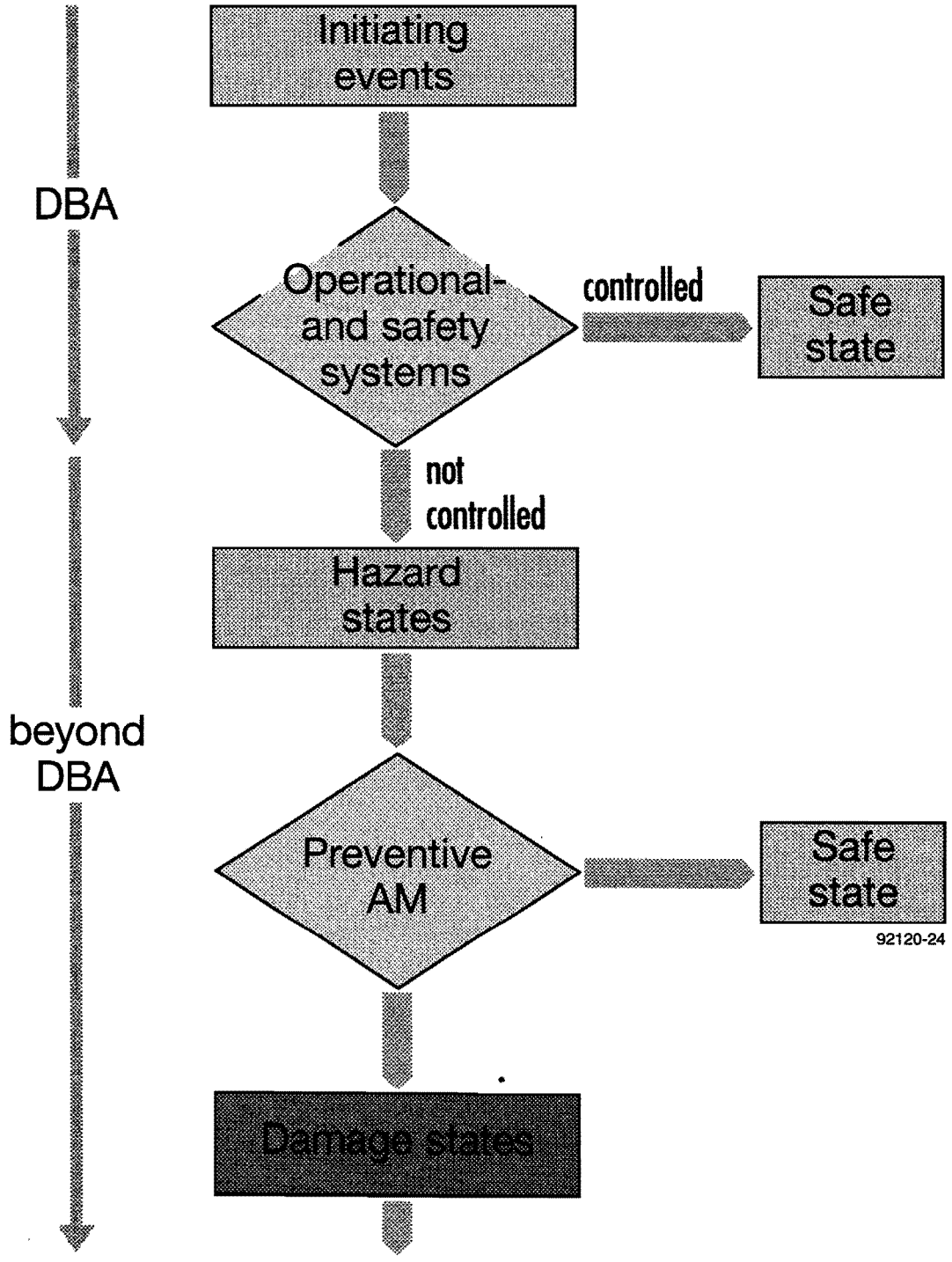


Figure 1-1 Hierarchy of Hazard and Damage States

2 Reference Plant Gundremmingen (KRB)

The reference plant for the present study is the Gundremmingen nuclear power plant (KRB), consisting of two units of 1300 MWe (KRB B) and 1308 MWe (KRB C) respectively, each equipped with a boiling water reactor of the 72 series serving as nuclear steam generator.

The plant was built by Kraftwerk Union AG (KWU). It is operated by RWE Energie AG and Bayernwerk AG. The two units were built right next to the Gundremmingen A nuclear power plant (250 Mwe) which was operated from 1966 to 1977. Unit B was commissioned in 1984, unit C in 1985.

2.1 Plant Design and Functions

Figure 2-1 shows the design and function of the reactor cooling system.

Inside the reactor core, heat is generated particularly through fission of the nuclear fuel and through radioactive decay. This heat causes part of the cooling water flowing through the reactor core to evaporate. The steam at a pressure of approx. 7 MPa is used to drive the turbo generators (3,4,5). On leaving the turbine the steam is condensed in the condenser (8). The condensate passes through a purification system and a pre-heater system (10) and is then pumped by the condensate pumps (9) into the feedwater tank (11) and by the feedwater pumps (12) into the reactor pressure vessel. The heat is removed from the condenser (8) via the main feedwater system (14-16). The heat is released mainly into the atmosphere via the cooling towers (16), and a small amount directly into the river.

2.2 Safety Concept

During operation, considerable amounts of radioactive substances are formed inside the nuclear power plant. The safety concept guarantees through the retention of these radioactive substances that a release of these substances to the environment is avoided or kept within permitted limits.

The decay of the radioactive substances formed during operation continues to generate heat (decay heat) even after shutdown of the reactor. Compared with the heat that is generated during operation, decay-heat production is small and decreases in the course of time. If, however, there were no cooling of the reactor core, the decay heat would be sufficient to heat up the reactor core to such an extent that radioactive substances could be released. Thus, it is necessary to continue cooling of the reactor core after shutdown.

The physical and technical operating conditions require the fulfillment of the following safety objectives:

- reactivity control:
  it must be possible to shut the reactor down at any time and to keep it in shutdown state;

- core cooling:
  core cooling must be guaranteed for every operational plant state; long-term reactor-core cooling and residual-heat removal must be guaranteed even after the reactor has been shut down;

- retention of radioactive substances:
  radioactive substances must be retained within the safety barriers.

The fulfillment of these safety objectives is ensured by a safety concept which provides several barriers for the safe retention of the radioactive substances inside the plant and by safety provisions and measures to protect these barriers.

The barriers are:

- the gas-tight fuel-rod cladding
- the reactor pressure vessel with the closed reactor-cooling circuit
- the containment with the containment penetrations.

In order to protect the barriers, staggered measures are used which correspond to different levels of defence.

On the first level, the quality of design, manufacture, construction and operating contribute to the achievement of consistent availability through undisturbed operation.

On the second level, the plant is kept within design-basis limits in case of operational disturbances with the help of control and limitation devices in order to avoid accidents.

On the third level, safety systems are provided to protect the barriers against the effects of a variety of accidents. The safety systems are designed redundantly (more systems than necessary) or sometimes also diversely (of differing design). They are automatically actuated and are controlled in such a way that for design-basis accidents manual intervention by the operating personnel does not become necessary earlier than 30 minutes after the onset of the accident.

Plant-dynamic investigations show that even after failure of the safety systems, the barries are threatened in most cases only after a longer period of time. This time can be used for accident-management measures, which form a fourth level.

2.3 Safety-relevant Systems

The following is a short description of the most important engineered safeguards; a survey is given in Figure 2-2.

The reactor-scram system serves for the quick interruption of the chain reaction and for the re-establishment of sub-criticality.

The nuclear residual-heat-removal system (Figure 2-3) comprises three trains. A diverse, additional residual-heat-removal and injection system (ARHR) (Figure 2-5) and a modified shutdown line on the level of the feedwater-line nozzles (Figures 2-3 and 2-4) are presently under construction. The nuclear residual-heat-removal system (Figure 2-4) comprises the following system functions: high-pressure injection, low-pressure injection, and suppression-pool cooling. Its task is among other things the long-term residual-heat removal after reactor shutdown via the nuclear cooling-water system and the nuclear service-water system. If coolant is lost it also has to feed water into the reactor-cooling system.

The automatic pressure limitation (Figure 2-6) has to limit the pressure increase in the reactor if the flow of steam from the reactor to the turbine is interrupted through isolation of the main-steam lines. The steam produced by the residual heat after reactor scram is discharged into the pressure-suppression pool via the eleven safety and relief valves (S+R valves) or via the three diverse pressure-relief valves which are located on the main-steam lines inside the wetwell, where it finally condenses.

At low RPV water level, for example, due to failure of HP-injection, the automatic pressure suppression with the relief valves lowers the pressure in the reactor-cooling system such that core cooling can be maintained through the low-pressure trains of the residual-heat-removal systems.

The pressure-suppression system (Figure 2-7) reduces the pressure build-up in the containment in the case of breaks of a main-steam or feedwater line. In this case, the steam entering the containment flows via vent pipes into the pressure-suppression pool; here it is condensed.

In the case of e.g. a break of a main-steam line outside the containment, the penetration-isolation valves shut off the main-steam line immediately before and behind the containment penetration.

The reactor protection system monitors all safety-relevant data and on reaching limit values actuates reactor-protection signals that initiate automatic protective actions.

The electric-power supply consists of the power system for house load and the emergency-power system. The power system for house load supplies the operational and safety-related components and systems. If the power for house load is lost, the safety-relevant components are supplied by the emergency-power system. For this purpose, there is an automatic switch to the 110 kV stand-by supply or to the emergency diesels.

2.4 Changes to the Systems and to the Operating Manual

In the following, the most important changes to the systems and to the operating manual are listed which were considered during the investigations. Partly, they were suggested by the analysis.

2.4.1 Changes Considered during the Systems Analysis

The following changes were made before the investigations were completed:

- direct connection of the pressure-suppression/feedwater system (RM/RL):
  use of the supply of condensate for feeding the RPV at failure of the main feedwater pump
- operation of a high-pressure-injection pump (TH 14) without low-pressure stage:
  I&C-actuation has been demeshed and separate cooling system for HP-injection pump installed
- cooling of pressure-suppression pool (PSP):
  actuation of operational PSP-cooling by all sub-system controls
- reduction of interlocking time from 30 to 5 minutes for reactor protection to shut down the residual-heat-removal pumps and maintain the supply of coolant within the containment
- possibility of reactivating the feedwater pumps at low feedwater level
- assurance of feedwater supply (RL) at failure of the main heat sink:
  shut-off of RL-system feeding at failure of PSP water-level control only if at least one of the residual-heat-removal systems is working
- depressurisation of RPV:
  manual depressurisation of RPV at high PSP-temperature (60 °C) only if RPV feed is ensured.

The following changes (as at 4/92) are to be operating as indicated:

- bypass valves:
  diverse valves for pressure limitation; realised in 1992

- modified shutdown line:
  additional shutdown line on the level of the feedwater-line nozzles in a residual-heat-removal train; consequently, possibility of shutdown according to operating manual at leaks in main-steam lines in the turbine building and at failure of steam-line isolation; realised in 1992

- ARHR-system:
  diverse residual-heat-removal and injection system; planned to be operating in 1994/1995.

2.4.2 Considered Changes Related to Carrying out Accident-Management Measures According to the Accident-Management Manual

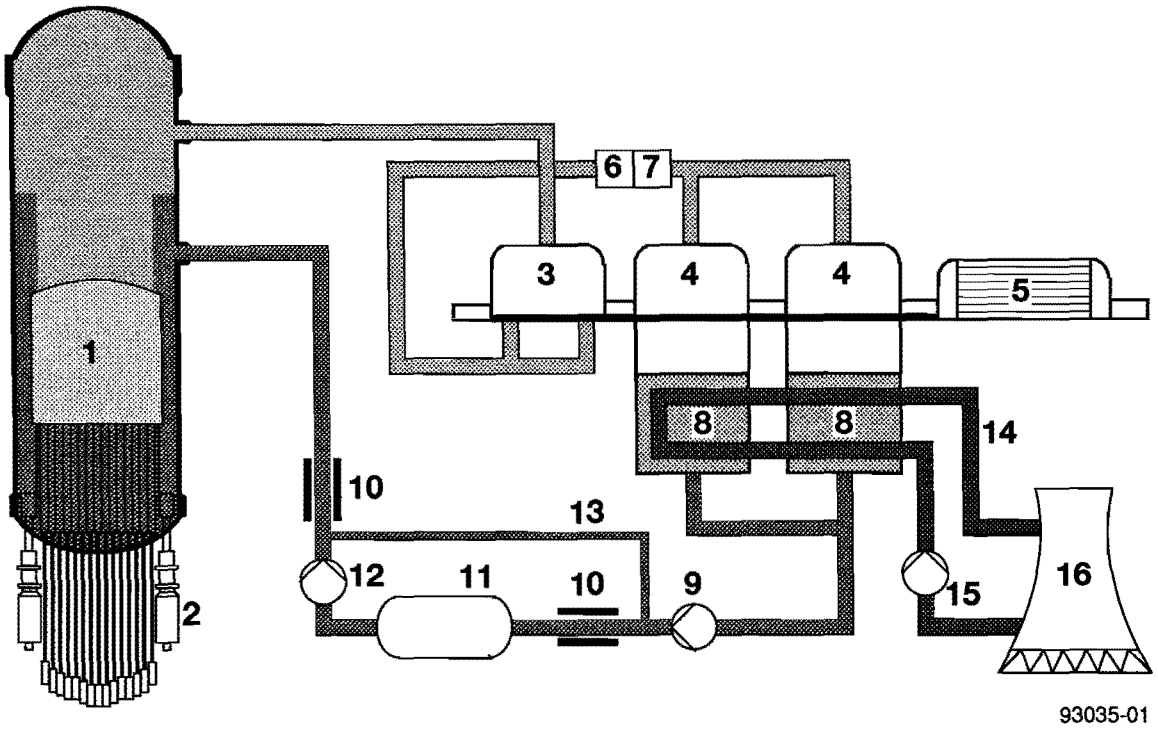
- Modified shutdown line:
  use of the modified shutdown line according to the accident-management manual at leaks in main-steam lines inside the reactor building and at failure of steam-line isolation; realised in 1992

- RPV-feeding:
  increased feeding with control-rod purge-water system and pump-seal-water system; already implemented
  feeding with fire-fighting system; already implemented
  direct feeding of water from the Danube with the service-water system; already implemented

- emergency power supply:
  cross-ties of AC-buses within the unit and between units; already implemented
  additional underground cable for the supply of the emergency AC-buses; realised in 1992

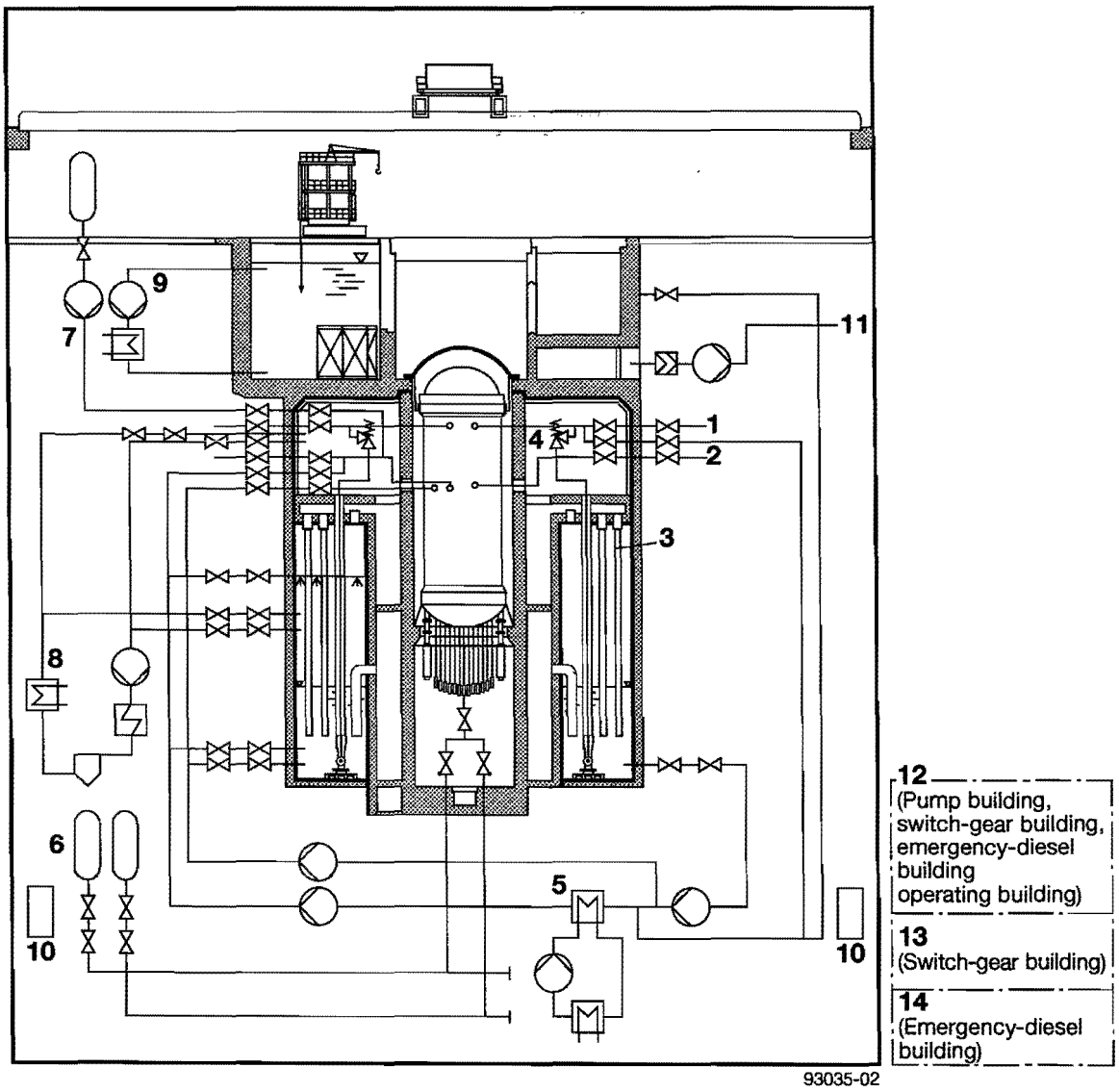
- residual-heat removal:
  filtered containment venting; already implemented

- mitigation measures; already implemented
  filtered containment venting
  inerting of wetwell
  filtering of control-room ventilation.



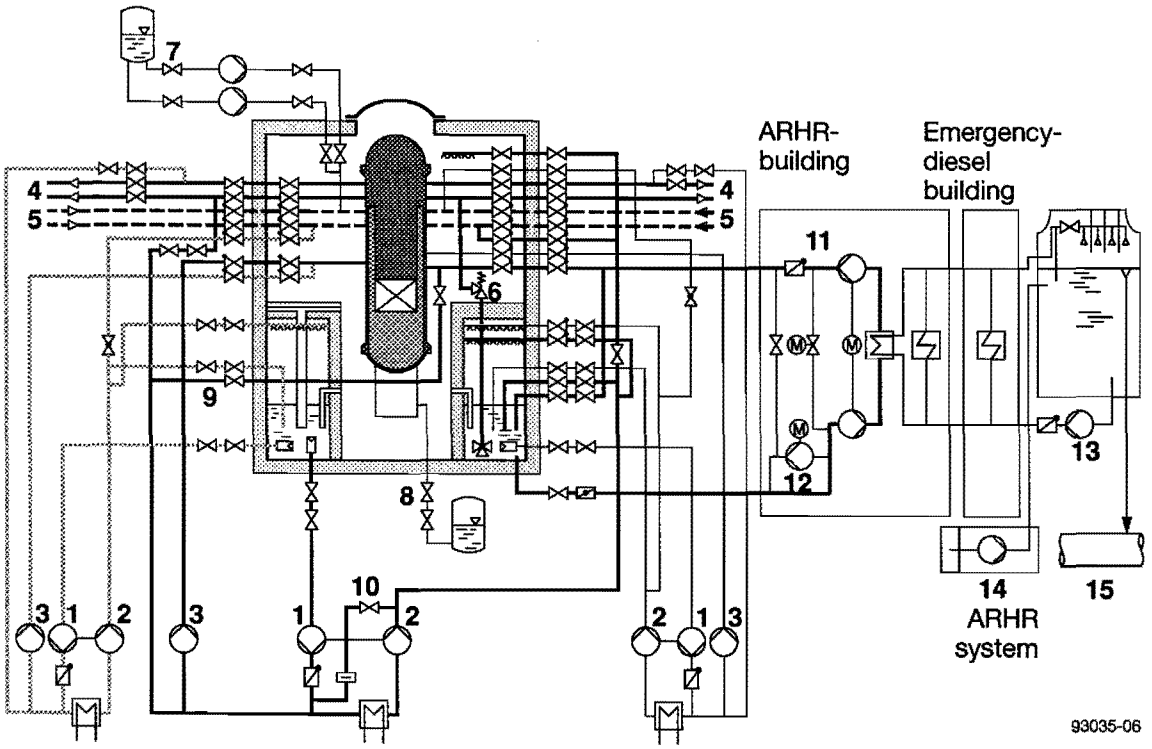
1 Reactor core
2 Main coolant pump
3 HP-part of turbine
4 LP-part of turbine
5 Generator
6 Water separator
7 Superheater
8 Pressure-suppression pool
9 Condensate pump
10 Pre-heater
11 Feedwater tank
12 Feedwater pump
13 RM/RL-interconnecting pipe
14 Cooling water
15 Cooling-water pump
16 Cooling tower

Figure 2-1 BWR, Basic Scheme of the Reactor-Cooling System



1 Main-steam line penetration valves
2 Main feedwater line penetration valves
3 Pressure-suppression system
4 Pressure-suppression system with safety & relief valves
5 RHR and closed-cooling-water system
6 Reactor-scram system
7 Borating system
8 Hydrogen-removal system
9 Fuel-storage-pool cooling system
10 Reactor protection (partial control points)
11 Sub-atmospheric pressure-holding system
13 Reactor protection (switch-gear building)
14 Emergency-diesels

Figure 2-2 KRB II: Engineered Safeguards



1 Pre-stage } LP-pump
2 LP-stage }
3 HP-pump
4 Main-steam lines
5 Feedwater lines
6 Pressure-suppression system
7 Borating system
8 Reactor-scram system
9 Modified shutdown line
10 Minimum-flow bypass
11 Feed pump
12 Filling pump
13 Service-water pump
14 Additional water pump
15 Drain channel

Figure 2-3 KRB II: Residual-Heat-Removal Systems

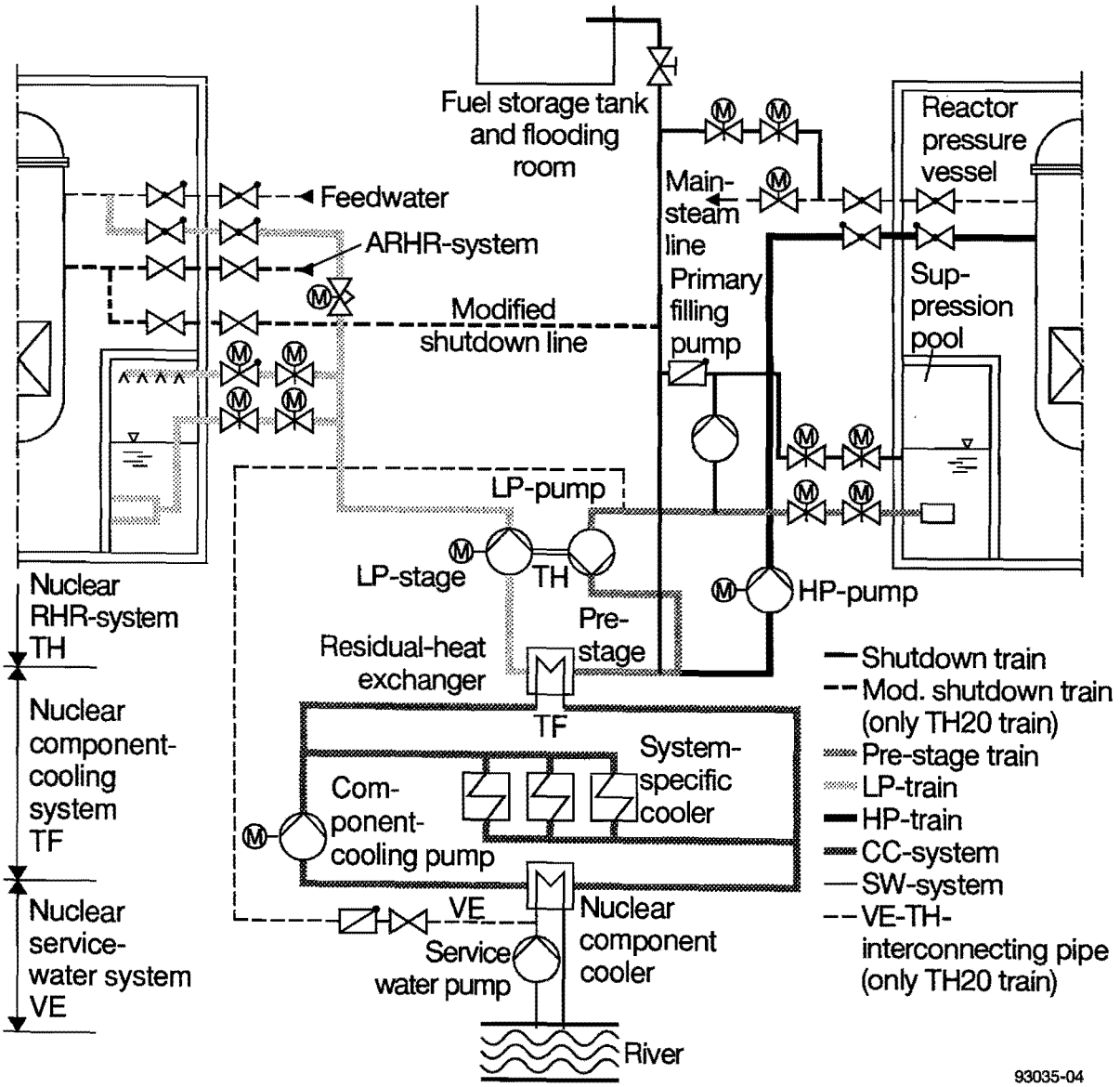


Figure 2-4 Residual-Heat-Removal Chain

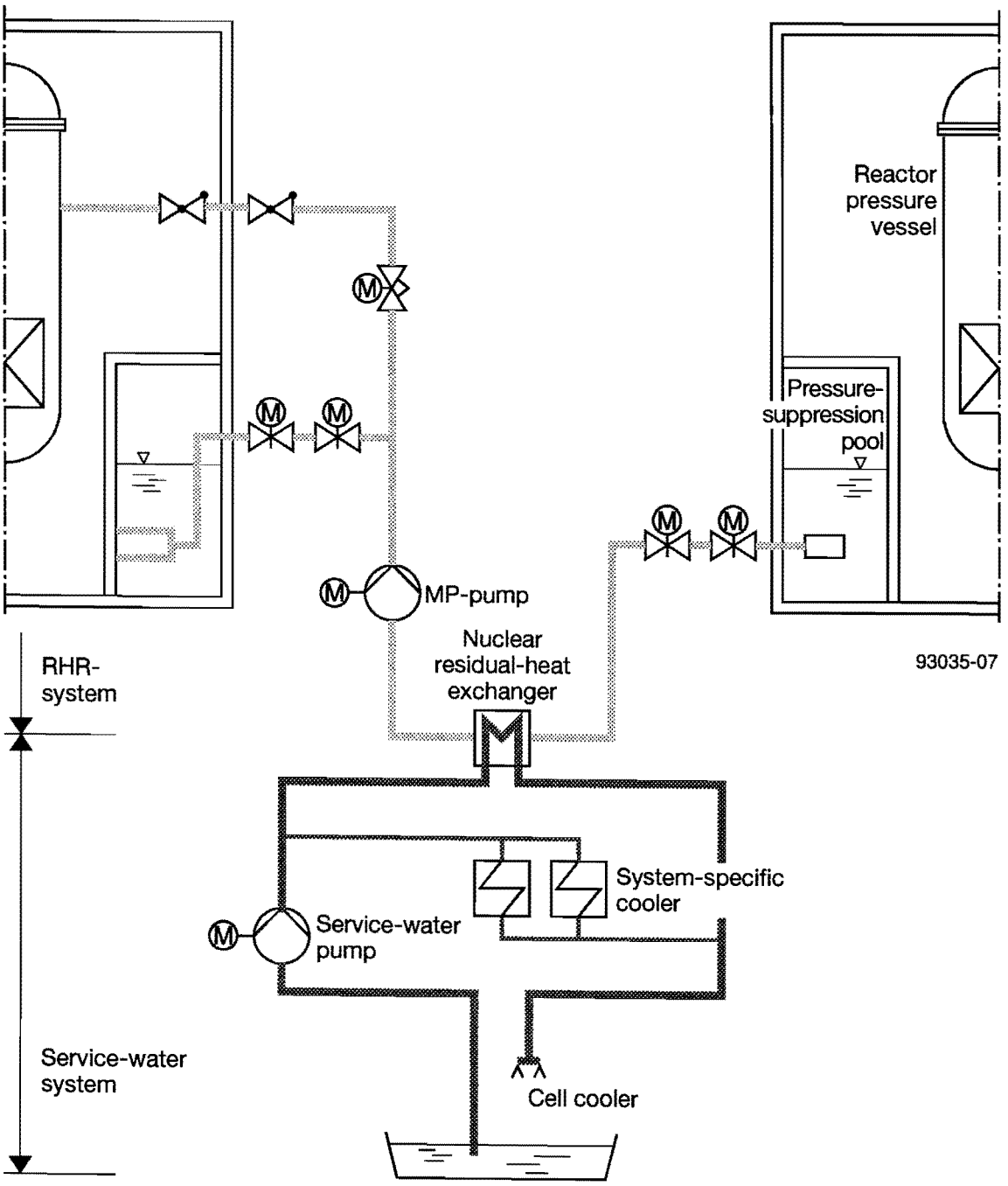


Figure 2-5 KRB II: Additional Residual-Heat-Removal and Injection System (ARHR)

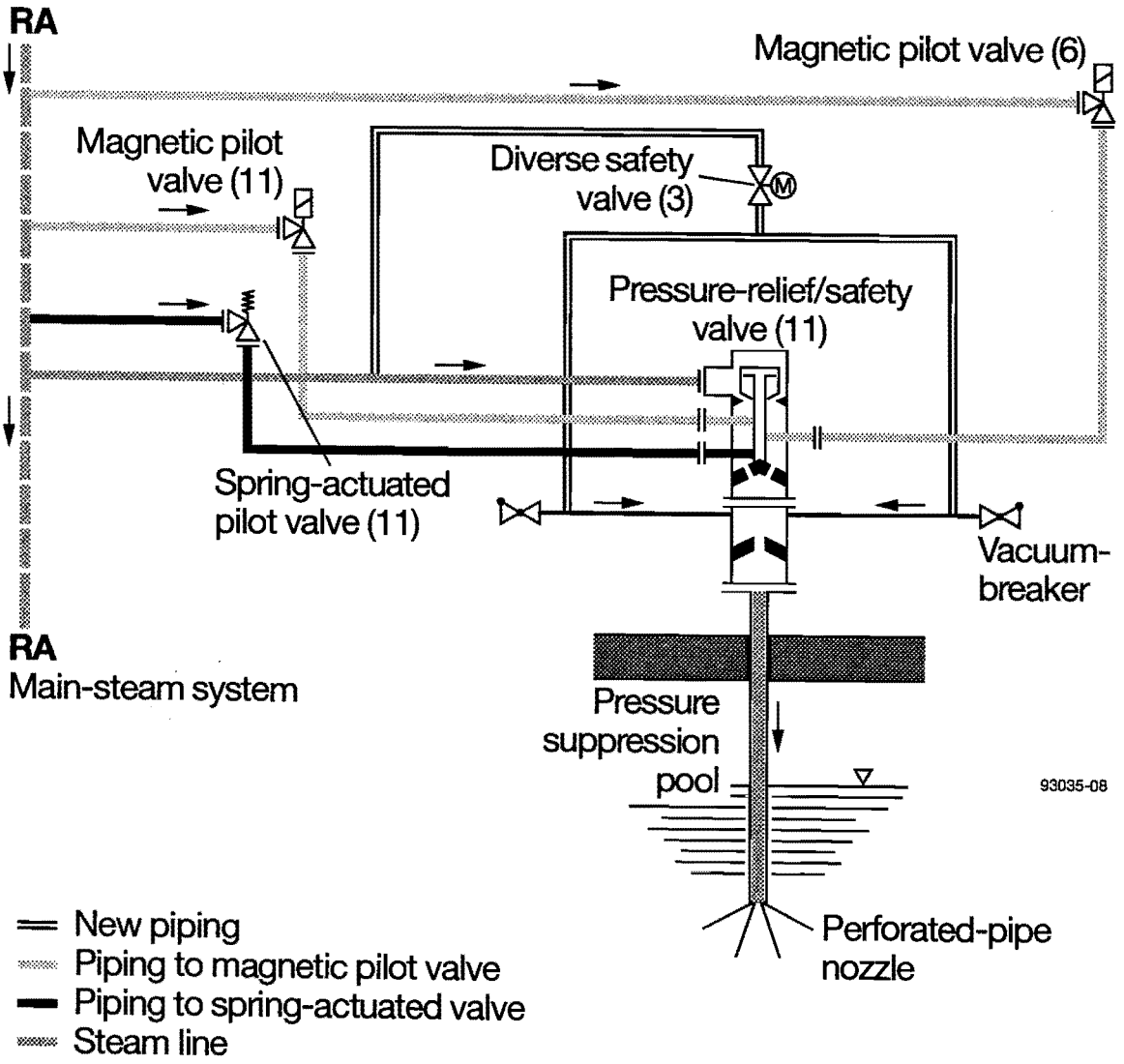
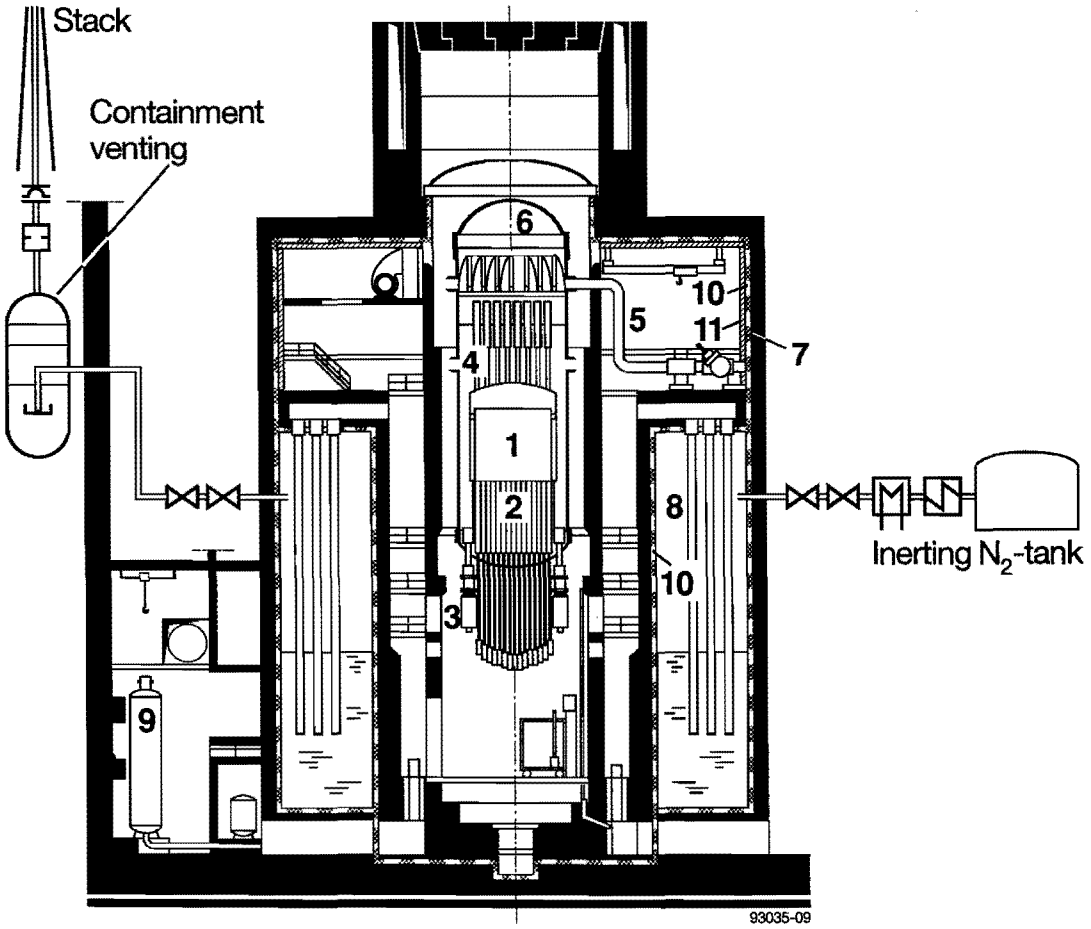


Figure 2-6 KRB II: Safety and Relief Valve, Diverse Pressure-Limitation Valve



1 Fuel elements
2 Control rods
3 Main coolant pumps
4 Feedwater nozzle
5 Main-steam line
6 Reactor pressure vessel
7 Containment
8 Pressure-suppression pool
9 Scram accumulator tank
10 Liner (sealing steel shell)
11 Missile-shielding concrete

Figure 2-7 KRB II: Longitudinal Section of the Containment with Pressure-Suppression System

3 Initiating Events

Upsets and damages of components or parts of the plant which trigger off safety systems are called "initiating events".

This analysis only looks at a limited number of initiating events. It makes a distinction between plant-internal events and plant-internal and plant-external common-cause initiators (CCI).

3.1 Groups of Events

- Plant-internal events

The investigated plant-internal events have been categorised in the following groups of events:

- operational transients
- transients caused by leaks in the RHR-system
- anticipated transients without scram (ATWS)
- leaks within the containment
- leaks outside the containment

The following initiating events belong to the groups of events:

- operational transients
  - loss of preferred power
  - loss of main feedwater
    (without failure of main heat sink)
  - failure of main heat sink
    (without loss of main feedwater supply)
  - failure of main heat sink and loss of main feedwater due to common cause

- failure to close of a safety and relief valve
- excess-feeding transient
- inadvertant opening of a turbine or bypass valve

- transients caused by large and small leaks in the RHR-system outside the containment

- anticipated transients without scram (ATWS)

- leaks within the containment:
  - small leak feedwater line
  - medium-size leak feedwater line
  - large leak feedwater line
  - small leak main-steam line
  - large leak main-steam line
  - RPV-bottom leak

Leaks in the feedwater and main-steam lines comprise leaks in these lines themselves and in those pipe sections that connect to the reactor cooling system and cannot be isolated. With these types of leaks the leaking coolant flows over into the pressure-suppression pool and thus becomes available for residual-heat removal.

This study does not deal with large leaks of the reactor pressure vessel as these are highly unlikely to occur.

- Leaks outside the containment:
  - small leak feedwater line
  - large leak feedwater line
  - small leak main-steam line
  - medium-size leak main-steam line

- large leak main-steam line

Leaks of pipes connecting to the reactor cooling system outside the isolating valve are not considered (with the exception of the RHR-system)

- Common-Cause Initiators (CCI)

These are groups of events which can have an impact on several safety installations at the same time:

- Plant-internal CCI
  - flooding
  - fire
- Plant-external CCI
  - earthquake
  - others (airplane crash, flooding due to high tide, explosion blast wave, impacts from the neighbouring unit)

For the groups of events, the following are considered as initiating events:

- Flooding
  - leak of the service-water system within the reactor building with flooding of safety systems
- Fire
  - transients through oil and cable fires in the control-rod-drive chamber within the containment
- Earthquake
  - leaks in the main-steam lines outside the containment following the collapse of the roof of the turbine building at an earthquake.

3.2 Frequency of Initiating Events

Table 3 lists the initiating events with their expected frequencies.

The expected frequencies of operational transients is determined by plant-specific operating experience of both units (total monitoring period of approx. 12 years of operation), using the Bayes approach without previous information. For the emergency power case a value has been estimated on the basis of zero-failure statistics.

The expected frequency of anticipated transients without scram (ATWS) is the result of the product of all expected frequencies of transients and the failure probability of reactor scram depending on the number and the combination of unavailable control rods. The failure probability is determined on the basis of national and international operating experience, using the Binominal-Failure-Rate (BFR) Model. German operating experience has shown failures of control-rod bulk insertion due to mechanical and electrical causes, although without negatively influencing fast rod insertion. Failure of the control-rod mechanism at fast rod insertion have occurred at two plants abroad, in each case at one individual rod.

Leaks have not occurred in the reference plant, although there have been some in other German BWR plants. The frequencies for small leaks up to 10 cm^2 within the containment are estimated on the basis of the operating experience of all German BWR plants. For determining the frequencies of leaks > 10 cm^2, this analysis uses the methodology developed in the German Risk Study Phase B (DRS-B) /1/ for pressurised water reactors. As there is only relatively little operating experience with German boiling water reactors it is necessary that future work go further than just using purely statistical data and include in the methodological investigation possible crack-formation mechanisms under the special conditions of the BWR water chemistry. Due to the high quality standard for pipes of the reactor cooling system, extremely low frequencies of < 10^{-7}/a are estimated for leaks > 500 cm^2.

For determining the expected frequencies of fires and the reliability data for fire-protection measures, available data relating to the operating experience of nuclear and conventional power stations is used. Generic and plant-specific values are employed for determining fire frequencies in different areas and reliability data for

fire-protection measures. Furthermore, the frequency of oil leackages is determined, and the conditional ignition probability is estimated.

A fire in the lower drywell of the containment can have an impact on many safety systems. Automatic pressure suppression and possibly also RPV water level measuring are the main functions that can be affected. Then, the expected failure rate of these functions is the result of the frequency of fires and the failure probability of the fire protection measures. A frequency of $< 3 \cdot 10^{-5}$/a is estimated for transients through fire within the containment.

The expected frequency of flooding within the reactor building is determined from the expected frequency for a large leak in the nuclear service-water system and the conditional probability of the safety systems within the reactor building being flooded during power operation. A frequency of $< 10^{-7}$/a is estimated for an event of this kind.

The expected frequencies for earthquakes of various intensities are determined by use of local seismic analyses. This results in earthquake-related probabilities of damages to the turbine building and therefore in upper bounds for the expected frequencies of larger leaks in the main-steam lines outside the containment ($< 6.3 \cdot 10^{-5}$/a).

The expected frequency of an airplane crash onto the reactor building is determined by use of crash statistics for military aircraft at $< 6 \cdot 10^{-7}$/a. Considering the design of the reactor building, the frequency for penetration of the reactor building as consequence of an airplane crash is $< 3 \cdot 10^{-8}$/a.

Table 3-1 Initiating events and frequencies

	Event		Expected frequency/ year
Operational transients			
T3	Loss of main heat sink		0.5
T3T2	Loss of main heat sink and loss of main feedwater due to common cause		0.3
T2	Loss of main feedwater		0.2
T5	Excess-feeding transient		0.2
T6	Inadvertant opening of turbine or bypass valve		0.2
T4	Failure to close of a safety and relief valve		0.1
T1	Loss of preferred power		0.04
Transients due to leaks in RHR-system			
T7	Leaks in RHR-system outside containment		
	small leak		$\sim 10^{-3}$
	large leak		$< 10^{-4}$
ATWS			
	Transients with loss of hydraulic injection and failure of electric drives		$< 10^{-7}$
	Loss of main heat sink with failure to initiate reactor scram		$1.0 \cdot 10^{-6}$
	Transients with depressurisation with mechanical failure of 2 or 3 adjacent control rods due to common-cause failure		$4.0 \cdot 10^{-5}$
	Transients with mechanical failure of 4 or more adjacent control rods due to common-cause failure		$3.0 \cdot 10^{-5}$
Leaks inside containment			
LI1-RL	Small leak in feedwater line	5 - 150 cm^2	$3.1 \cdot 10^{-3}$
LI2-RL	Medium-size leak in feedwater line	150 - 300 cm^2	$9.0 \cdot 10^{-5}$
LI3-RL	Large leak in feedwater line	$\geq$ 300 cm^2	$< 10^{-7}$
LI1-FD	Small leak in main-steam line	5 - 50 cm^2	$4.3 \cdot 10^{-3}$
LI3-FD	Large leak in main-steam line	$\geq$ 300 cm^2	$< 10^{-7}$
LIB	RPV-bottom leak		not assessed

Table 3-1 Initiating events and frequencies (continued)

Event			Expected frequency/ year
Leaks outside containment			
LA1-RL	Small leak in feedwater line	5 - 150 cm^2	$9.1 \cdot 10^{-3}$
LA3-RL	Large leak in feedwater line	$\geq$ 300 cm^2	$3.5 \cdot 10^{-4}$
LA1-FD	Small leak in main-steam line	5 - 50 cm^2	$2.9 \cdot 10^{-3}$
LA2-FD	Medium-size leak in main-steam line	50 - 300 cm^2	$1.9 \cdot 10^{-4}$
LA3-FD	Large leak in main-steam line	$\geq$ 300 cm^2	$< 5 \cdot 10^{-7}$
	Interfacing systems LOCA		not assessed
Internal flooding			
	Leak in service-water cooling system inside reactor building and failure to trip the pumps		$< 10^{-7}$
Fire			
	Transients caused by fire		$< 3 \cdot 10^{-5}$
Seismic events			
	Leaks in main-steam line outside containment caused by failure of turbine building due to earthquakes		$< 6 \cdot 10^{-5}$
	Transients and LOCA caused by earthquakes		$< 6 \cdot 10^{-7}$
Others			
	Aircraft crash with penetration of the reactor building		$< 10^{-7}$
	Events caused by flood, blast wave, impacts from the neighbouring unit		$< 10^{-7}$

4 Analyses of Event Sequences

For controlling an initiating event, the following operational or safety systems are required in order to maintain

- sub-criticality,
- core cooling and
- retention of radioactivity.

The operational and safety system have to fulfil different functions which are called system functions. They also contain manual actions by the operating personnel in accordance with the operating manual. The minimum requirements to the system functions are detemined by thermohydraulic and neutron-physical analyses. If the minimum requirements are not met, the result may be a hazard state.

4.1 System Functions for Controlling Accidents[1]

For maintaining sub-criticality, *reactor scram* is necessary. It interrupts the nuclear chain reaction and brings the plant to a "sub-critical, hot" state.

The maintaining of core cooling normally requires *automatic pressure limitation* in the RPV and sufficient RPV-feeding. *Automatic pressure limitation* has to keep the pressure in the RPV below the feed pressure of high-pressure injection. For this purpose there are 11 safety and relief valves and, in addition, 3 diverse bypass valves available.

For RPV-injection, the system functions *HP-injection* and *LP-injection* are available.

HP-injection is possible by using the

- main feedwater system or the
- HP-pumps of the nuclear RHR-system.

These systems can feed the RPV at high as well as at low pressure.

[1] The system functions are printed in italics.

The pump-seal-water and control-rod-purge systems continually inject small amounts of coolant into the RPV; in most of the accident processes considered here they are, however, not capable of keeping up a sufficiently high water level in the RPV.

At failure of HP-RPV-injection, the sinking of the water to a very low level automatically actuates *depressurisation* and *LP-injection* (RPV-flooding). For automatic *depressurisation,* six safety and relief valves are available. In addition, a further relief valve can be opened manually.

LP-injection can be performed with the low-pressure systems of the nuclear RHR-system; medium-pressure injection can be carried out with the ARHR-system (planned to be operational in 1994/95). In some cases, RPV-injection is also possible with the condensate pumps via a bypass line and also by passive draining of the feedwater tank. There furthermore are other injection possibilities in the framework of accident-management measures.

At high RPV-pressure and failure to trip the HP-injection systems, the functioning and integrity of the safety and relief valves may be put at risk by blow-down of sub-cooled water. Damage to the S+R valves can be avoided by the system function *excess-feeding protection.* This comprises all the measures which avoid the required use of S+R valves at high pressure and extremely high RPV water level.

For preventing excess feeding of the main-steam lines and the auxiliary steam lines outside the containment at RPV-flooding and possible consequent failure of these lines, the system function *steam-line isolation at excess feeding* is activated. In case of a failure of the steam-line isolation during excess feeding of the main and auxiliary steam lines, these lines are flooded outside the containment. The main and auxiliary steam lines as well as the connecting systems are not designed to withstand the resulting dynamic loads. A failure of these lines is, however, not necessarily to be presumed. If the main and auxiliary steam lines should be able to cope with the resulting loads, the failure of the *steam-line isolation at excess feeding* would have no effects. There are at present no analytic models available for determining the load acceptance at excess feeding of the main-steam lines. More comprehensive model developments and analyses would be necessary for a more detailed determination of the failure probability of these lines.

At excess feeding with failure of the main-steam line, core cooling can be maintained with the planned "modified shutdown line" (to be operational in 1992) which can remove the residual heat even at a water level below the main-steam-line nozzles. In case of a break situation in the turbine hall, residual-heat removal can be performed in accordance with the operating manual. In case of a break situation in the reactor building, additional measures in accordance with the accident-management manual are necessary.

Residual-heat removal can be performed either via the main heat sink (turbine and condenser) or via the nuclear RHR-chain from the pressure-suppression pool or directly from the RPV.

Residual-heat removal from the pressure-suppression pool and the RPV is performed via the LP-trains of the nuclear RHR-system, via the nuclear closed-cooling-water system to the nuclear service-cooling-water or the additional RHR-system (ARHR).

Failure of the system function *residual-heat removal* results in a temperature and pressure increase in the containment. In this case, the removal of heat into the atmosphere and thus a limitation of pressure and temperature inside the containment is still possible by filtered depressurisation of the containment (accident-management measure).

4.2 Minimum Requirements for System Functions

The following describes the minimum requirements that the system functions have to meet in order to control initiating events. It furthermore indicates how many of the sometimes multiply available system trains or partial systems are required to fulfil the system functions.

- *Reactor scram*

  For maintaining sufficient sub-criticality, 192 of 193 control rods must in the most unfavourable case be hydraulically fast inserted or electrically inserted at "cold, xenon-free" plant state. *Reactor scram* has failed for the "hot" plant state if four or more adjacent control rods - or more than four, depending on the combination of failure positions - are not inserted. At loss of the main feedwater supply *reactor*

scram is only actuated if certain RPV-water-level values are reached. In all other cases there are at least two diverse actuation criteria available for *reactor scram*.

- *Automatic pressure limitation*
  For successful pressure limitation it is necessary to open
  - 1 of 11 safety and relief valves, or
  - 2 of 3 of the diverse bypass valves.
- *Injection with HP-systems*
  Necessary are
  - 1 of 3 main feedwater pumps, or
  - 1 of 3 HP-pumps of the RHR-system;

  with the operation of the HP-pump also being possible in one of the three trains without the LP-pump as a booster pump
- *Depressurisation*
  For achieving RPV-flooding with the LP-pumps of the RHR-system it is necessary to have
  - 2 of 7 S+R valves in open position.

  For feeding with the ARHR-system it is necessary to have
  - 1 of 7 S+R valves in open position, or
  - 2 of 3 bypass valves in open position.
- *Injection with LP-systems*
  Necessary in the function RPV-flooding are
  - 1 of 3 LP-pumps of the RHR-system, or
  - 1 of 1 ARHR-system.
- *Residual-heat removal*
  Necessary for limiting the temperature of the pressure-suppression pool water to a level below 150 °C are

- 1 of 3 residual-heat-removal trains via the pressure-suppression-pool cooling line or RPV-feeding, or
- 1 of 3 residual-heat-removal trains via the minimum-flow line, or
- 1 of 1 ARHR-system, or
- 2 of 2 service pumps of the RHR-system via the pressure-suppression pool cooling line or the LP-minimum-flow line at RPV-injection with TH14 or
- 3 of 3 service pumps at RPV-injection with the main feedwater system.

The requirements for the service pumps took into account that the temperature in the pressure-suppression pool must not exceed 100 °C (max. permissible operating temperature of the service pumps). For safeguarding the operation of the HP-pumps of the RHR-system within the design scope, the temperature must be kept below 85 °C. For this particular case, higher requirements are necessary for *residual-heat removal.*

- *Steam-line isolation at excess feeding*
  Necessary are
  - closing of 1 of 2 isolating valves in each main-steam line, or
  - cut-off of injection at extremely high RPV water level.
- *Steam-line isolation of main-steam lines*
  At leak of a main-steam line outside the containment:
  - closing of 1 of 2 isolating valves in the main-steam line affected by the leak.
- *Steam-line isolation of feedwater lines*
  Necessary is the check-valve function of
  - 1 of 2 isolating valves in each feedwater line.
- *Excess-feeding protection*
  Necessary are:
  at excess feeding with the main feedwater system
  - cutting-off of the main feedwater system

  at sustained water level with the HP-pumps of the RHR-system:

- cutting-off of all excessively feeding HP-injections, or
- opening of 2 of 3 bypass valves.

At RPV-flooding:
- opening of 1 of 7 S+R valves, or
- opening of 3 of 3 bypass valves.

4.3 Event Sequences

Detailed analyses were only carried out for events during power operation. Event-sequence diagrammes were drawn up for the investigated initiating events; they served as a basis for the analyses of the systems. The most important event sequences are illustrated by the example of the transient "loss of main heat sink".

Starting from the initiating event, the event sequences are followed up until either the sequence is classified as controlled or a plant hazard state occurs. The plant hazard states are marked by characteristic plant states and by the time spans until they occur. The plant states are classified as follows:

- b_1 Resulting from the failure of residual-heat removal, the temperature in the pressure-suppression pool exceeds 150 °C.
  Above this temperature it is not possible to operate the residual-heat-removal system. Below this temperature RPV-feeding is not endangered. By heat-up and partial dryout of the pressure-suppression pool, pressure and temperature increase in the containment whose integrity will be challenged after approx. 10 h.

- b_2 In the case of failure of the steam-line isolation and RPV-feeding not being cut off, the RPV water level exceeds the level of the main-steam lines. This entails a failure of the steam line or of the adjacent systems.
  The loss of coolant after an assumed failure of the steam line leads to a rapid drop of the water level of the pressure-suppression pool and after 2 hours at the earliest to a hazard to core cooling.

- b_2^* The RPV water level of the pressure-suppression pool falls below the normal level by more than 6.5 m due to a leak in a main-steam line outside the containment and failure of steam-line isolation and subsequent evaporation of the coolant.
  In this plant state core cooling would be challenged after 2 days at the earliest.

- b_3 The RPV water level reaches the bottom of the core due to failure of RPV-feeding.

- b_4 The RPV-pressure exceeds the design pressure by a factor of 1.3 (approx. 12 MPa) as a result of the failure of the pressure limitation of the reactor cooling circuit.

To further characterise the state of the plant, the analysis differentiates between low pressure (LP), i. e. after depressurisation, and high pressure (HP) in the RPV when the hazard occurs.

A simplified event-sequence diagramme for the loss of the main heat sink is shown in figure 4-1. The hazard states are given for the end of each event path. The indicated periods mark the earliest possible points in time at which the respective hazard states are reached. The closure of the S+R valves and the feeding with the direct RM/RL-connection are not considered since a failure of these functions does not lead to the development of any totally new event sequences.

For controlling the transient, *reactor scram* and *automatic pressure limitation*, RPV-feeding (possibly with previous *depressurisation*), *residual-heat removal* and, in case of excess feeding, *steam-line isolation of the main-steam line* are necessary.

The effects of the failure of system functions necessary for controlling accidents are described in the following:

- *Reactor scram*

Failure of *reactor scram* leads to an ATWS-case (path 16). This case is investigated separately.

- *Automatic pressure limitation*

At failure of the *automatic pressure limitation* there is a rapid build-up of pressure inside the RPV, exceeding the feed pressure of the HP-systems. If the pressure increases further to above approx. 12 MPa, the integrity of the pressurised components of the reactor-cooling system is at risk.

- *Injection with HP-systems*

This function comprises RPV-feeding with the main feedwater system or the HP-pumps of the RHR-system in the operating modes 'maintaining of water level' or 'RPV-flooding'. For reasons of a simplified presentation in the summary, this function was treated together with the corresponding *excess-feeding protection*.

At failure of *injection with HP-systems* the RPV water level will sink. Sufficient feeding of the RPV can then be performed by the LP-systems after depressurisation has been carried out. The failure of HP-feeding alone does not lead to a hazard state (path 7).

- *Residual-heat removal*

The system function *residual-heat removal* is necessary for controlling each initiating event considered here. Its failure always leads to hazard states with plant states of the category b_1 (paths 3 to 6 and 11 to 14). After exceeding the maximum permissible temperature (approx. 85 °C) of the pressure-suppression-pool water, the HP-pumps of the RHR-system will be lost for further RPV-feeding (paths 3 to 6). After RPV-depressurisation has taken place, RPV-feeding can for some time be upheld with the LP-pumps of the RHR-system. A failure of the pumps is presumed at a temperature of the pressure-suppression-pool water of 150 °C (design temperature of the LP-pumps). This temperature, combined with a pressure of approx. 0.5 MPa inside the containment, is reached approx. 10 hours after the onset of the accident (paths 3 and 11).

- *Depressurisation*

Depressurisation is necessary in order to feed the RPV after a loss of the HP-injection systems with the LP-pumps of the RHR-system or with the ARHR-system. Provided that these systems as well as residual-heat removal and steam-line isolation function normally, the transient is controlled (path 7).

If *depressurisation* fails, LP-injection is not possible. The coolant inventory will evaporate, and the result will be a hazard state at high RPV-pressure (paths 6, 10, 14).

- *Injection with LP-systems*

If *depressurisation* is functionning normally, RPV-feeding can be performed with the LP-trains of the RHR-system or with the ARHR-system.

If *injection with LP-systems* fails, the coolant supply of the RPV will evaporate, and the result will be a hazard state at high RPV-pressure with plant states of the category b_3 (paths 5, 9, 13). For paths 9 and 13, *injection with HP- and LP-systems* is not available from the start. Thus core cooling is at risk after a relatively short (approx. 30 min.) period of time (b_3).

The moment of the onset of the hazard state can be delayed through injection via the direct RM/RL-connection from the pressure-suppresion pool into the RPV. Due to the limited amount of condensate available, injection of this kind cannot be sustained for long. It has therefore not been included in the simplified diagramme.

- *Steam-line isolation at excess feeding*

Steam-line isolation of the main-steam lines is required if the RPV is flooded with HP-injection after the failure to maintain the water level or in case of unwanted excess feeding.

If the *steam-line isolation* fails, the affected main-steam lines outside the containment are flooded. If this leads to a leak in the main-steam line or the connecting systems, a hazard state of the category b_2 will occur (paths 2, 4, 8, 12). If the injections into the RPV can be interrupted after the leak has formed - which at failure of RPV water level

measuring can only be achieved through accident-management-manual measures - it is possible in the case of a break situation in the turbine hall to control the state described here by using the planned shutdown line in accordance with the operating manual and, in other break situations, to control it according to the accident-management manual. At failure of measures for using the shutdown line, a hazard state of the category b_2* will occur after between 30 min and several days, depending on the moment when RPV-injection is cut off.

4.4 Thermodynamic Investigations

For determining the effectiveness of system functions, thermodynamic investigations were carried out with the ATHLET code.

The case of loss of preferred power with loss of the emergency-power supply was selected as representative transient involving drop of the RPV water level because this case has high demands on the safety systems and neither the main heat sink nor the main feedwater supply are available. The sequence described in the following is also valid for the loss of the main heat sink up until the start of the draining of the feedwater tank into the RPV. This study furthermore investigated the effectiveness of passive draining of the feedwater tank into the RPV which can be performed without applying any further measure only in the case of loss of preferred power.

The case of loss of preferred power is triggered off by the failure of the station-service supply (10-kV-house-load busbar). The emergency AC-buses are designed to be supplied through reactor-protection actuations by the 110-kV-emergency-power supply. If this supply of the emergency AC-buses is lost, the start-up and connection of the emergency diesels is automatically activated. The additional failure of all emergency diesels and of all manual actions results in a station blackout.

As soon as there is a loss of preferred power, turbine trip is triggered. Up to four S+R valves will open simultaneously, activated by the turbine-trip signal. At the same time, the bypass-control valves to the condenser will open and bring the system pressure to normal. Four S+R valves will close within 4-10 seconds. After approx. 12 seconds the oil pressure which controls the opening position of the bypass-control valves is reduced to such an extent (no emergency-power supply for the control oil pumps) that

they will close by themselves. Consequently, the pressure in the RPV increases and activates reactor scram. After reactor scram has been activated, the system pressure increases further and is limited by the S+R valves. Then the RPV water level decreases due to the mass flow out of the RPV via the S+R valves.

The further description of the sequence is based on calculations with the ATHLET code for the "station blackout" sequence.

Feeding with the RHR-systems is actuated 24 seconds after the onset of the accident by the low RPV water level; it does, however, not become effective due to the lacking power supply. After approx. 400 seconds, automatic pressure-suppression is triggered off at very low RPV water level. At first, two S+R valves open; another four S+R valves open with a delay of 200 seconds.

Approx. 12 minutes after the onset of the accident, the system pressure falls below the saturation pressure in the feedwater lines. Through evaporation of the coolant in the feedwater lines approx. 60,000 kg of coolant are forced into the RPV. This causes a temporary rise of the RPV water level (see Figure 4-2). After approx. 22 minutes, the system pressure has decreased to such an extent that the saturation pressure in the feedwater tank is also reached and that further injection from the feedwater lines or the feedwater tank takes place. There are further injections from the feedwater tank, decreasing in the amount of water being injected. After approx. 55 minutes, RPV-feeding is ended. During the first hour after the onset of the accident, a total amount of 300,000 kg of water is fed from the feedwater tank and feedwater line into the RPV. During this process the RPV water level is almost brought back to normal.

After approx. 150 minutes, the RPV water level (Figure 4-2) has sunk through evaporation to such an extent that the core begins to heat up. At this point, approx. 430,000 kg of coolant have evaporated: approx. 67 % through decay heat, approx. 20 % through evaporation due to depressurisation, and approx. 13 % through structural heat release.

The analysis of the case of loss of preferred power shows that the reservoirs of coolant from the feedwater tank and the feedwater line can be used to a large extent if the S+R valves are fully available. Core heat-up only begins approx. 2 1/2 hours after

the onset of the accident. RPV-injection by active systems must begin no later than at this point in order to avoid damage to the core.

At loss of the main heat sink with loss of RPV-feeding there is no draining of the feedwater tank into the RPV because of the pressure decrease caused by the spraying of condensate into the feedwater tank. In this case, core heat-up would already begin after approx. 30 minutes.

4.5 Events outside Power Operation

For events outside power operation there were only scoping analyses carried out. They showed that the analyses can be very complex and comprehensive due to conditions that are specific to outage periods. Therefore further, more detailed and systematic studies are necessary in order to be able to make a comprehensive assessment of events outside power operation.

These investigations considered events during

- shutdown of the plant for unplanned outages and
- inspection outage of the plant for refuelling.

Accident-management measures were not taken into account. The studies differentiated between four phases, marked by different plant states.

The results are summarised as follows:

- Phase I: Shutdown of the plant via turbine and bypass-control valves, RPV isolated

  In principle, the same event sequences are possible in this operational phase as during power operation. The following event sequences are considered important:

  - water-level transients caused by too little RPV-feeding or too high steam discharge
  - pressure transients caused by too little steam discharge.

Compared with power operation, an increased frequency for these events must be reckoned with in this operational phase. In contrast to power operation, however, the progress of these transients is slower.

- Phase II: Residual-heat removal via the residual-heat-removal chain, RPV isolated

  For this operational phase, the following events are investigated:

  - failure of components in the residual-heat-removal chain
  - failure of the steam-line isolation of the main-steam line
  - leak in the residual-heat-removal chain outside the containment.

These event sequences have in common that in case of a malfunction in the removal of residual heat there is a pressure build-up in the reactor due to the fact that it is still isolated and that residual-heat removal via pressure-relief valves is possible by feeding steam into the pressure-suppression pool and by RPV-feeding to compensate for evaporated water.

- Phase III: Residual-heat removal via the residual-heat-removal chain, RPV open, reactor well not flooded

  For this operational phase the following events were investigated:

  - failure of components in the residual-heat-removal chain
  - failure of the steam-line isolation of the main-steam line.

These event sequences have the special operational states of the RHR-systems in common that are caused by the RPV-excess-feeding protection. Due to the opened RPV-lid there is no pressure build-up possible in the RPV; it may, however, be that the water in the reactor heats up to boiling point and evaporates from the open RPV into the reactor building.

- Phase IV: Residual-heat removal via the residual-heat-removal chain, reactor well flooded, suction from dryer and separator-storage pool

  For this operational phase the following events were investigated:

  - failure of components in the residual-heat-removal chain

- leakage of the flooding compensator
- failure of plugs or plates during work on primary isolation valves
- load crash onto the RPV
- leak in RPV-bottom
- loss-of-preferred-power case
- reactivity events and maloperations during core loading.

Due to the inert system behaviour there is enough time available for counter-measures in the event of "failure of components in the residual-heat-removal chain". Similar event sequences occur in the two leak-accident cases "leakage of the flooding compensator" and "failure of plugs or plates". It is typical of these events that the lower part of the reactor building is flooded if the main hatches fail to close. The possibilities and the success of the necessary immediate measures for the leak-accident cases depend on the time available and therefore on the size of the leak.

For the event "failure of plugs or plates", the failure of the plate of a feedwater nozzle was investigated. The resulting event sequences largely compare with those of a large leak in the flooding compensator. Any differences are mainly due to the fact that the RPV water level sinks lower than in the case of a flooding-compensator leak and that the open primary isolation valves must first be closed and the reactor must be re-flooded before the decay heat can be removed with the RHR-system.

As the relevant event for a load crash onto the RPV, the effects of a crash of the heaviest-possible component, the RPV-lid (115,000 kg), was investigated. The estimations made in this context showed that the support structure may be plastically deformed but that the pipes connecting to the RPV remain unaffected. Therefore the crash of the RPV-lid onto the RPV is not considered to be relevant.

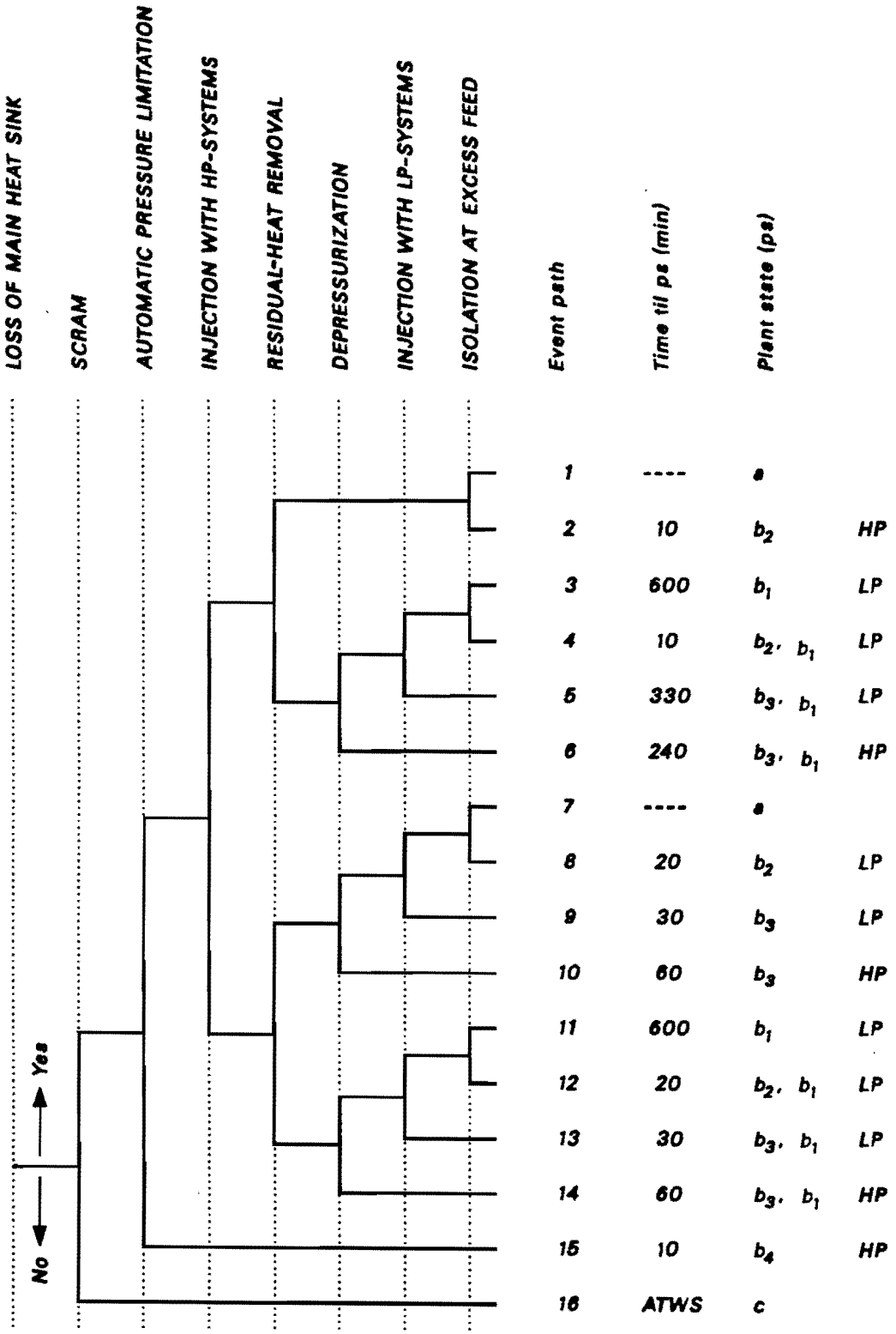
The event "leak in RPV-bottom" can occur through leakages at the penetrations of the main coolant pumps, control-rod drives and instrument lances. As the seals at these penetrations are of similar design, a leakage at the largest penetration (main coolant pump) was investigated as representative event.

The initiating event selected for the investigations of the case of loss of preferred power was the loss of the supply from the grid with regard to various states of the power-supply (cut-off). There is a long time span available until the onset of the hazard state caused by loss of power.

- Reactivity and loading accidents

In the context of reactivity accidents, the faulty withdrawal of control rods at zero load (start-up accident) is of special importance here. Under conservative assumptions the investigations showed that especially in combination with maloperations during core loading, prompt critical states cannot in principle be excluded, even during inspection outages, i.e. with the RPV open. In this context it was presumed that the central control rod was withdrawn and the four control rods next to it were being withdrawn together. The prerequisite for this is the simultaneous occurrence of several failures or maloperations by the operator. Without a more detailed analysis, taking into account the heat-up of the coolant and the dynamics of steam formation, it is not possible to say to what extent the power increase - at presumed failure of reactor scram - can lead to damage of the affected fuel elements. It would be sensible especially for the core-loading phase to safeguard reactor scram at faulty withdrawal of a control rod not only through the actuation by the intermediate-range detector probes but additionaly through a further actuation (e.g. by the start-up-range detector probes).

If computer programmes are used for drawing up the plan for the core-loading procedure it may in particular happen that a systematic error at the input of data related to the burn-up-dependent process of reactivity or to the required sub-criticality can lead to a range of maloperations during core loading with the consequence that a sufficient shutdown margin is not maintained any more even with the control rods fully inserted. The possibility of such errors might be reduced through diverse ways of controlling the sub-criticality of each core-loading step, e.g. through checking the data for burn-up of adjacent fuel elements.



a	*transient controlled*
b_1	*suppr.-pool temp. > 150 C due to failure of residual-heat removal*
b_2	*excess feeding without isolation and failure of steam line*
b_3	*RPV water level < bottom of core*
b_4	*RPV-pressure > 1.3 times design pressure (approx. 12 MPa)*
c	*transition to ATWS*
HP	*high pressure (no RPV-depressurisation)*
LP	*low pressure (after RPV-depressurisation)*

Figure 4-1 Loss of the main heat sink (simplified diagramme)

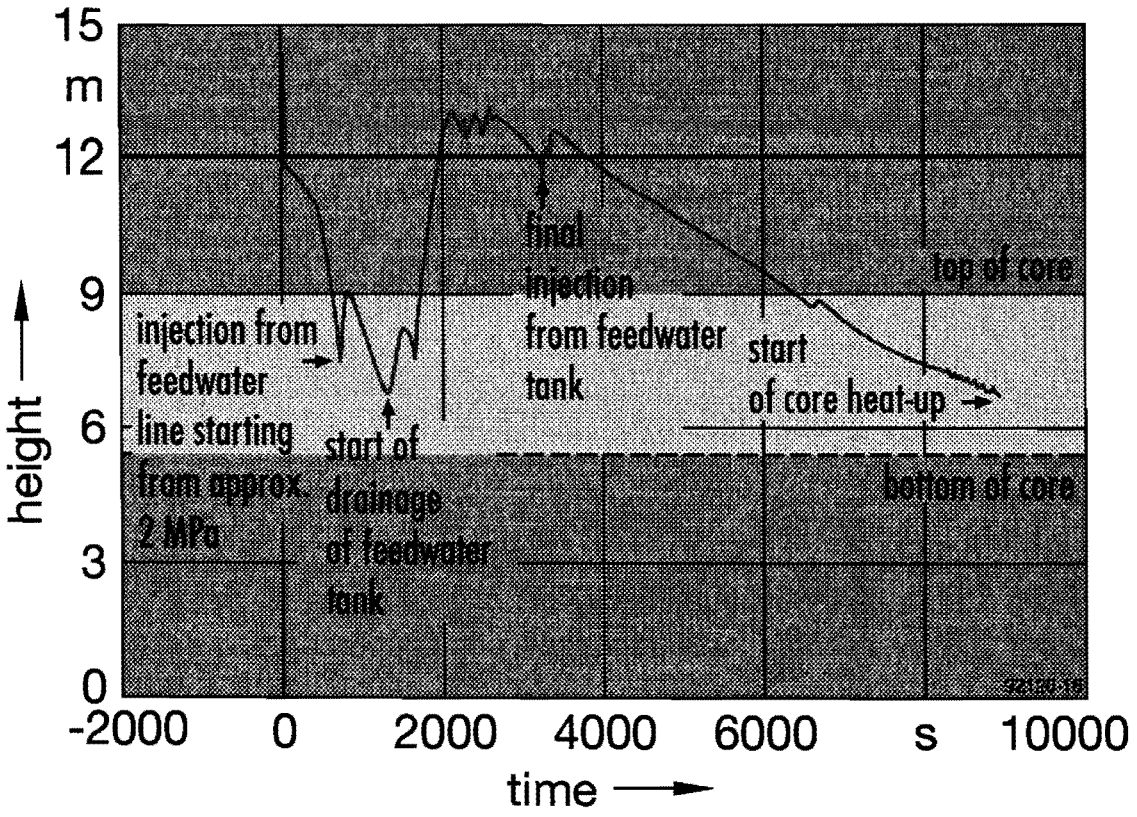


Figure 4-2 Loss of preferred power with use of feedwater system (RL); hight H (m) of the reduced RPV water level

5 Systems Analyses

For the determination of the frequency of hazard states, the corresponding mean unavailabilities of the system functions were determined by means of fault-tree analyses carried out for the systems relevant to process engineering, electrical systems and instrumentation and control. Fault-tree analyses identify the relevant combinations of system failures that can lead to a hazard state. In this context, information is required concerning systems configuration, operating instructions (operating manual, test and inspection manual), results from event-sequence analyses as well as reliability data for components and actions taken by the operating personnel.

5.1 Reliability Data

5.1.1 Independent Failures

Depending on the failure mode, reliability data are required for components related to process engineering, electrical systems, and instrumentation and control. The twin-unit plant of Gundremmingen consists of the identical units B and C and some installations utilised by both units. The two units went into operation with approx. 8 months between them. The systems technology of both units is largely identical and built up from components made by the same manufacturer. Maintenance of both units is carried out by the same maintenance team, and the same maintenance strategy is applied.

Extensive data acquisition was conducted in both units. In both units there was a sufficient database for the components; only in some individual cases did the evaluation of data result in any significant differences in the failure characteristics of components. Due to the generally good coincidence of the failure characteristics of components and due to the identical design of the components, the data from units B and C was merged in a common plant-specific database, thus broadening the database.

For those components of which no plant-specific data could be acquired, data compiled in other nuclear power plants in the Federal Republic of Germany was used.

For the selected data, the transferability was checked individually, taking into account important factors that can influence the failure characteristics.

5.1.2 Common-Cause Failures

The independent failure of systems with several (redundant) trains is highly unlikely. Failures caused by impact mechanisms which lead to the simultaneous failure of several trains due to common cause are more likely. They can significantly influence the reliability of systems. Therefore common-cause failures are taken into account and evaluated in the analysis.

There are the following kinds of dependent failures:

- Failure to function of several redundant components or partial systems, occurring as the consequence of one single failure. These are so-called 'causal failures'.
- Failure to function of several redundant components or partial systems, resulting from functional interdependences, i.e. from the system structure. There can, for example, exist functional dependences on one common support system, on one common drive mechanism or on human maloperations.
- Failure to function of several redundant components or partial systems of the same or similar design due to common, though undetected, causes.

The first two dependences are treated by the fault-tree analysis.

The third type of function failure from common cause is internationally known as 'common-cause failure' (CCF). Failures of this kind were modelled separately and taken into account in the analysis using special reliability data.

The evaluation of CCFs for the BWR safety analysis rests mainly on the work performed in the framework of the German Risk Study, Phase B (DRS-B). There has been no further development of the database.

Three sources of operating experience were evaluated in the framework of DRS-B with respect to CCFs. They were:

- OECD Incident Reporting System (IRS) reports, incorporating the experience of approx. 1000 reactor operating years
- reports on special events in the Federal Republic of Germany (events that must be reported), approx. 100 reactor operating years
- plant-specific evaluations from the reference plant Biblis-B, 3.75 reactor operating years.

The different models for quantification were assessed. A modified "Binominal-Failure-Rate (BFR) Model" formed the basis for the estimation of the necessary reliability parameters. Models like the Beta-Factor or the Multiple-Greek-Letter Model (MGM-Model) correlate the frequency of multiple failures with a factor to be determined from operating experience with the frequency of independent failures. For this purpose the correlation factors must be taken from the same data source as the frequency of independent failures. At the employment of plant-specific data for independent failures, the parameters for these models cannot be estimated satisfactorily. Thus they are less suited.

The following prerequisites or assumptions are to be taken into account at assessment and quantification:

- An estimation on the systems level is not possible because the systems generally cannot be compared.
- Estimations are made for groups of components because they offer a rather better scope for comparison which in turn can be better verified.
- For each relevant event mentioned in the given references the applicability and the transferability are technically assessed and the parameters of the BFR-model are estimated. For this purpose, the operating times of multiply available groups of components with the same characteristics are combined.
- The transferability is assessed considering the failure-detection probability in the reference plant.
- Uncertainty factors are estimated, with attention being paid to the compatibility of the upper bound values with the operating experience in the Federal Republic of Germany.

- In cases of high redundancy grades of components, limiting estimations are carried out if the application range of the modified BFR-model is exceeded.

CCF-probabilities on demand for some selected components are shown in Table 5-1.

Table 5-1 Selected reliability data for CCFs

Group of components	T_{CCF} (h)	Failure combi-nations	Failure mode	Failure probability (mean value)	K-Factor
220-V- or 24-V-battery incl. fuse	8 760	3 of 3	no voltage	$2 \cdot 10^{-5}$	12
Trip unit	8 760	for a threshold value	wrong adjustment	$3 \cdot 10^{-5}$	12
RPV water level measurement devices	672	8 of 9	no measured value	$5 \cdot 10^{-6}$	12
Emergency diesel GY10-30D101	672	3 of 3	does not start	$3 \cdot 10^{-4}$	7
ISO valves RA01-41S101/102	8 760	> 4 of 10	do not close	$1.5 \cdot 10^{-4}$	12
TF-cooler TF10-30B101/102	200	3 of 3	no heat transferral	$1.4 \cdot 10^{-6}$	7
HP-injection pump TH14-34D101	420	3 of 3	does not start	$3.7 \cdot 10^{-5}$	7
LP-RHR pump TH13-33D101	200	3 of 3	does not start	$1.6 \cdot 10^{-5}$	7
Component-cooling pumps TF10-30D101	168	3 of 3	does not start	$1.5 \cdot 10^{-5}$	7
Service-water pumps VE10-30D101	168	3 of 3	does not start	$1.5 \cdot 10^{-5}$	7
Gate valve TH13-33S202	200	3 of 3	does not open	$3.6 \cdot 10^{-5}$	7

T_{CCF}: Failure-detection time

K-Factor: Quotient from 95 %- and 50 %-fractile

5.1.3 Treatment of Manual Actions

Planned manual actions by plant personnel for accident management were identified and analysed. The fault trees consider only those manual actions whose failures have relevance to the investigated event sequences. The investigations only took those manual actions into account which are part of operating routine or which are laid down in the operating manual.

In order to be able to determine which of the identified manual actions have a significant influence on the unavailabilities of the respective system functions, screening values were employed as the basis for the failure probabilities linked to these manual actions; these screening values are in turn based on the results of the "Accident Sequence Evaluation Program - Human Reliability Analysis Procedure (ASEP)" /2/. Table 5-2 shows a selection of the failure probabilities for manual actions as they were used in the fault-tree calculations. Failure probabilities of 0.08 were used in cases of "critical actions with moderately high level of stress". For manual actions estimated as "critical actions with extremely high levels of stress" there is a screening value of 0.4 according to ASEP. A failure probability of 1 was assumed for a diagnosis of the plant state and the execution of manual actions with very little time (approx. 10 min) available.

Table 5-2 Selected failure probabilities for manual actions (screening values)

Description of manual action	Failure probability (mean value)
Start-up of residual-heat removal	0.08
Re-set of reactor-protection signal after activation	0.08
Cut-in of emergency diesels	0.4
Cut-in of RPV-feeding before the core is uncovered (at failure of RPV water level measuring)	0.4
Additional feeding of water into the pressure-suppression pool before the criteria for manual initiation of main-steam-line isolation are reached	0.4
Cut-in of RPV-feeding before the threshold value "RPV water level very low" ("LT3") is reached	1

5.2 Results of the Systems Analyses

Table 5-3 shows the results of the systems analyses of the considered plant-internal events. It contains the various initiating events and their frequencies, the relevant hazard states and their frequencies, and the conditional mean unavailabilities of the system functions at the transition stage between initiating event and hazard state. In Table 5-3 as well as in Figures 5-1 and 5-3 the events are shown without consideration of the ARHR-system and the modified shutdown line. Table 5-4 and Figures 5-4 to 5-6 show the results with these system changes taken into account.

The abbreviations used in the tables have the following meanings:

T1 = Loss of preferred power
T2 = Loss of main feedwater supply
T3 = Loss of main heat sink
T3T2 = Loss of main heat sink and loss of main feedwater supply due to common cause
T4 = Failure to close of a S+R valve
LA1-FD = Small leak in main-steam line outside containment
LI1-FD = Small leak in main-steam line inside containment
LI1-RL = Small leak in feedwater line inside containment
ATWS = Loss of main feedwater supply with failure of the initiation of reactor scram
HP = High pressure in RPV (no RPV-depressurisation)
LP = Low pressure in RPV (after RPV-depressurisation)

The frequency of a hazard state is the result of the multiplication of the frequencies of an initiating event with the corresponding mean unavailabilities of system functions. The fault trees were evaluated for the determination of the mean unavailabilities of the system functions. The evaluation was carried out with the RALLY code package, using an analytic simulative procedure for the determination of the minimal cuts. Minimal cuts in this context are defined as those component combinations in the fault tree whose simultaneous failure is just enough to cause a system failure. The mean unavailability is then calculated by means of the determined failure combinations. The table shows the totals of the mean unavailabilities of the system functions for the corresponding hazard states.

The results do not contain the frequencies of hazards at plant states b_2 or b_2^* with transients and loss-of-coolant accidents inside the containment because the behaviour of the main-steam lines and the connecting systems after excess RPV-feeding with failure of the steam-line isolation (and water flow into these lines) was not assessed. More detailed plant-specific investigations are necessary for a corroborated quantification of the failure probabilities of the main-steam lines and the connecting systems. This is also the reason why the excess-feeding transient T5 could not be assessed.

Three important initiating events were selected from the range of loss-of-coolant accidents (cf. Table 3-1) and were subsequently assessed. The small leak in a feedwater line outside the containment was not analysed. The following paragraphs look at the frequencies of hazard states and the unavailabilities of the system functions for the individual initiating events.

- Transients
- Loss of preferred power (T1)

Point value of the expected total frequency of the hazard states: $3.2 \cdot 10^{-6}$/a.
Mean unavailability of the system functions: $8.0 \cdot 10^{-5}$.

In approx. 94 % of the cases the mean unavailability is characterised by failures which lead to the failure of RPV-feeding (plant state b_3). Approx. 6 % can be put on failures of residual-heat removal which leads to a temperature increase in the pressure-suppresion pool to more than 150 °C (plant state b_1). The failure of RPV-pressure limitation (plant state b_4) with less than 1 % is negligable for the case of loss of preferred power.

Approx. 55 % of the unavailabilities of the system functions can be put down to component failures of the nuclear closed-cooling-water system (TF-system), the nuclear service-water system (VE-system) and the nuclear residual-heat-removal system (TH-system), with the following predominant failure combinations:

- Failure to start of the 3 of 3 pumps of the nuclear closed-cooling-water system or the nuclear service-water system due to common-cause failures

- Failure to start of the 3 of 3 LP-pumps of the RHR-system due to common-cause failure, at water temperature of the Danube higher than 10 °C.

The failure of all three closed-cooling-water-system pumps or of all three service-water-system pumps always leads to the failure of the entire RHR-system as well as to the failure of the LP-pumps and of 2 of 3 HP-pumps as a consequence of the lack of cooling of motors and bearings. The third HP-pump (train TH10) is cooled independent from the closed-cooling-water and service-water systems. However, a failure of this pump is still to be assumed due to the high temperature in the pressure-suppression pool. In case of the failure of all LP-pumps, high pressure-suppression-pool temperatures can be avoided by using the primary filling pumps if the water temperature of the Danube is below 10 °C. If the temperature is above 10 °C, the failure of all LP-pumps leads to the subsequent failure of all HP-pumps and consequently to the failure of all injections by the RHR-system. Since the main feedwater system is not available in the case of loss of preferred power, there is a failure of RPV-feeding (plant state b_3) at the onset of one of the above-mentioned common-cause failures of the pumps, in which case a hazard will occur after 5 hours at the earliest.

Approx. 35 % of the mean unavailabilities of the system functions are contributed by the failure of emergency-power supply; here, the largest share is taken by the common-cause failure of the 24-V-DC supply which leads to the failure to switch to the 110-kV-standby supply as well as to the failure to start up the emergency diesels. After about 60 minutes these failures lead to the uncovering of the core (plant state b_3) at high pressure.

- Loss of main feedwater supply (T2)

Point value of the expected total frequency of the hazard states: $5.5 \cdot 10^{-6}$/a.
Mean unavailability of the system functions: $2.8 \cdot 10^{-5}$.

As in the case of loss of preferred power, the hazard states that lead to a failure of RPV-feeding (plant state b_3) are dominant (approx. 91 %). The common-cause failures of the pumps as mentioned in connection with the case of loss of preferred power are decisive for the failure of RPV-feeding, even if the pump failures only lead to a hazard state if they occur in connection with an additional loss of the main heat sink. The loss of the main heat sink can mainly be put down to the failure of timely

feeding of water into the pressure-suppression pool (manual action) und the failure to open of the main-steam bypass station. If the feeding of water into the pressure-suppresion pool is not performed in time, the operating manual demands the isolation of the main-steam lines, which means that the main heat sink is no longer available. Here, plant state b_1 (temperature in the pressure-suppression pool > 150 °C due to failure of the RHR-system) also plays a subordinate role with only approx. 9 %. The possibility of the failure of RPV-pressure limitation (b_4) is negligable.

- Loss of main heat sink (T3)

Point value of the expected total frequency of the hazard states: $2.0 \cdot 10^{-5}$/a.
Mean unavailability of the system functions: $4.1 \cdot 10^{-5}$.

The result is dominated with approx. 96 % by the failure of the RHR-system (plant state b_1), which can be mainly put down to common-cause failures of the nuclear closed-cooling-water system and the nuclear service-water system. As a consequence of these failures, the temperature in the pressure-suppression pool reaches 150 °C after about 10 hours. Since in the case of this transient the main feedwater system can be used for RPV-feeding, plant state b_3 plays a subordinate role with only approx. 4 %. A hazard state through failure of RPV-pressure limitation (plant state b_4) is negligable for the result; it accounts for less than 1 %.

- Loss of main heat sink and loss of main feedwater supply due to common cause (T3T2)

Point value of the expected total frequency of the hazard states: $1.5 \cdot 10^{-5}$/a.
Mean unavailability of the system functions: $5.1 \cdot 10^{-5}$.

This result is determined by approx. 90 % through failures which lead to the failure of RPV-feeding (plant state b_3), with common-cause failures of the pumps (cf. case of loss of preferred power) having considerable importance. The remaining approx. 10 % are put down to the failure of the RHR-system (plant state b_1). The failure of RPV-pressure limitation plays, with less than 1 %, no significant role.

- Failure to close of a S+R valve (T4)

Point value of the expected total frequency of the hazard states: $1.5 \cdot 10^{-5}$/a.
Mean unavailability of the system functions: $4.1 \cdot 10^{-5}$.

As with the loss of the main heat sink (T3), the result is determined by the failure of the RHR-system (approx. 96 %) which after about 10 hours leads to plant state b_1 (temperature in the pressure-suppresion pool reaches 150 °C). The failure combinations correspond to those of T3. This is in principle also true of the failure of RPV-feeding (plant state b_3) which accounts for about 4 %.

- Loss-of-coolant accidents

- Small leak in main-steam line outside containment (LA1-FD)

Point value of the expected total frequencies of the hazard states: $2 \cdot 10^{-7}$/a.
Mean unavailability of the system functions: $7.2 \cdot 10^{-5}$.

Plant states b_1 and b_2^* are about equally affected. As with the loss of the main heat sink (T3), the main failure combinations which lead to plant state b_1 are the common-cause failures of pumps since the main heat sink is not available as a consequence of the activation of steam-line isolation in all main-steam lines. A failure of steam-line isolation in the main-steam line affected by the leak leads to a loss of coolant from the pressure-suppression pool. Here, the failure causes are mainly common-cause failures of the isolation valves. In connection with the failure to feed water into the pressure-suppression pool, a hazard state of the category b_2^* occurs after 2 days at the earliest. In this context, the operational RPV-injections through the control-rod-purge system and the pump-seal-water system are not taken into consideration, which leads to a pessimistic estimate.

- Small leak in main-steam line or feedwater line inside containment (LI1-FD, LI1-RL)

Point value of the expected total frequencies of the hazard states: $4 \cdot 10^{-7}$/a, $3 \cdot 10^{-7}$/a.
Mean unavailability of the system functions: $9.7 \cdot 10^{-5}$.

About 95 % of this result can be put down to the failure of RPV-feeding (plant state b_3) and about 5 % to the failure of the RHR-system (plant state b_1). The failure of RPV-pressure limitation (plant state b_4) is negligable.

The failure of RPV-feeding (b_3) is mainly caused by common-cause failures of all three motor-driven valves (does not open) in the minimum-flow lines of the LP-pumps of the RHR-system as well as by common-cause failures of the LP-pumps, the closed-cooling-water pumps, and the nuclear service-water pumps. If the motor-driven valves in the minimum-flow lines fail, a consequent failure of the LP-pumps is assumed as in this case the pumps will at times pump the coolant towards closed valves.

At the analysis of loss-of-coolant accidents it is assumed that the functioning of the RHR-system is not inhibited by loose isolation material as a consequence of the initiating events.

Possibilities of clogging of strainers were already considered in the design of the plant and were assessed to be irrelevant. More recent operating experience, however, questions the validity of the assumptions made at the design stage. This aspect and the possible consequences for the functioning of the RHR-systems could not be considered anymore in the framework of this analysis.

- Plant states b_2 and b_2^*

There would be additions to the total frequency of hazard states if it came to plant states b_2 or b_2^* due to excess-feeding of the RPV with consequent failure of a main-steam line or its connecting systems. The frequency increase is determined by the conditional failure probability of the lines.

The frequency of the event sequences involving excess feeding of the main-steam line which would lead to plant state b_2 as early as after approx. 10 minutes (least favourable case) is mainly determined by the transients. Dominant in this respect are the failures of the main feedwater supply (initiating events T1, T2, T3T2) as well as the excess-feeding transient T5, each case in connection with a failure of measured-data detection for the RPV water level due to common-cause failures. As a consequence, the feeding pumps could not be switched off at high RPV water level, nor could steam-line isolation be activated.

The frequency of the hazard states due to a fall below an extremely low water level in the pressure-suppression pool as a consequence of a leak in a main-steam line outside the containment caused by excess feeding (b_2*, onset after 2 days at the earliest) would mainly be determined by the leaks inside the containment with simultaneous failure of steam-line isolation.

- ATWS

Two different failure mechanisms were investigated which may lead to an ATWS event.

Case 1: Failure of reactor-protection-system activation for scram.

The determining factor for the unavailability of reactor-protection-system activation is the initiating event "loss of main feedwater supply" (frequency 0.2/a) where the scram signals are only generated by the RPV water-level-measurement device. The failure probability of the water-level-measurement device is $5 \cdot 10^{-6}$/demand (CCF of detection of RPV water-level-measurement device, cf. Table 5-1). The result for the frequency of this case is $1 \cdot 10^{-6}$/a (see Tables 5-3 or 5-4).

This case can only be managed if a scram and RPV-feeding are actuated manually before core damage occurs. The control room has indirect information about the water level in the core available through measuring of core temperature (presently in testing phase). It is furthermore intended to use an ultrasonic measurement technique as diverse RPV water level measurement. Even though there are further possibilities for state recognition available to the operator, like e.g. failure of RPV-feeding, the pessimistic assumption is made that due to the fast progress of this ATWS event manual actions will not be carried out in time with a probability of P = 1 and that for this reason the event cannot be controlled.

Case 2: Several adjacent control rods cannot be inserted either hydraulically or motor-driven. For these ATWS cases the reliability of the reactor-scram system was investigated.

- At the failure of two or three adjacent control rods, sub-criticality cannot be achieved at cold reactor state with transients involving pressure and temperature decrease in the RPV (frequency 0.2/a). The failure probability of the rod mechanics due to common causes is $1.8 \cdot 10^{-4}$/demand. The frequency of this event is thus estimated at $3.6 \cdot 10^{-5}$/a.

- At the failure of four or more adjacent control rods the hot, sub-critical reactor state cannot even be achieved in case of transients requesting reactor scram (frequency 1/a). The failure probability with a value of $2.9 \cdot 10^{-5}$/demand is determined by the CCF of four to seven adjacent control rods. The frequency of this event is thus $2.9 \cdot 10^{-5}$/a.

It was estimated that compared with a successful scram the requirements to residual-heat removal are slightly higher or reach a level up to that of decay heat, depending on the number of adjacent contol rods not being inserted. However, no detailed calculations were performed in this connection.

At the failure of eight or more adjacent control rods it is to be assumed that the capacity of the RHR-system will be exceeded. The frequency of such mechanical failure combinations cannot be sufficiently quantified with the BFR-model.

The two examined ATWS cases differ in their temporal development. Hazard states can occur in Case 1 after a short period of time. In Case 2 there is sufficient time for establishing sub-criticality through additional measures like e.g. borating. The further event sequence of the failure combination of Case 2 is still to be examined.

- Influence of the ARHR-system and the modified shutdown line

The results obtained under consideration of the planned ARHR-system and the modified shutdown line are shown in Table 5-4 and Figure 5-7. As the ARHR-system has not yet been realised, the evaluation of its reliability could only be made with the help of the design documents. Furthermore lacking is the plant-specific operating experience for the individual components of the system. It is planned to build components into the ARHR system which are designed diversely compared with the RHR-system so that the CCF of components of the RHR- and the ARHR-systems need not be assumed. On the other hand it is to be presumed that a CCF of the RPV

water-level-measurement device will also lead to the failure of the activation signals for the ARHR-system.

Analogous to Table 5-3, Table 5-4 does not contain any frequencies of hazard states at transients and loss-of-coolant accidents inside the containment which are marked by plants states b_2 or b_2^*.

In all, the installation of the ARHR-system reduces the total frequency of hazard states by a factor of 11. The most significant reductions of the unavailabilities of systems or of the frequencies are found for the hazard states involving loss of residual-heat removal (plant state b_1). The frequency of plant state b_1 is reduced from $2.6 \cdot 10^{-5}$/a (without ARHR) by a factor of almost 40 to $7 \cdot 10^{-7}$/a (with ARHR). At plant state b_3 the frequency is reduced by a factor of 7 to $3.4 \cdot 10^{-6}$/a. In this context it must be taken into account that the ARHR-system has no influence on the frequency of b_3 at ATWS (loss of main feedwater supply with failure of reactor-scram signals) because the CCF of the RPV water-level-measurement device also leads to the failure of the signals for RPV-feeding through ARHR. In the case of the remaining transients with loss of main feedwater supply, the contributions to the frequency of plant state b_3 (T1, T3T2) due to this CCF are also not reduced by the ARHR-system. In case of a loss of preferred power the 24-V or 220-V-DC supply failure through common cause (with additional failure of the manual action to start up the emergency diesels), the depressurisation required for feeding by the ARHR-system cannot be performed by automatic depressurisation. Therefore ARHR cannot become active despite its own diverse power supply. The ARHR-system has no influence on plant states of the b_2 and b_2^* categories.

- Influence of CCFs and failures of planned manual actions

Without considering ARHR and the additional shutdown line, CCFs contribute with approx. 99 % (in the sense of importance) to the total frequency of the hazard states. Failure combinations which exclusively contain CCFs contribute with approx. 80 % to the total frequency of the hazard states. About 60 % of the total frequency are caused by the failure to start of all three nuclear closed-cooling-water-system pumps as well as all three nuclear service-water pumps at accidents involving a loss of the main heat sink (frequency of the concerned initiating events approx. 1/a). In these cases, the failure of the nuclear component-cooling-water-system pumps or the nuclear

service-water pumps leads to a failure of residual-heat removal from the pressure-suppression pool as well as to consequent damage to the residual-heat-removal pumps due to the lack of cooling and therefore also to a hazard to core cooling. Thus, at events involving failure of main heat sink and functioning main feedwater system, there is a hazard resulting from the failure of residual-heat removal; this hazard is characterised by plant state b_1 (water temperature in the pressure-suppression pool exceeding 150 °C) and a very long period until its onset (approx. 10 hours). However, in the case of transients or loss-of-coolant accidents with unavailability of either the main heat sink or the main feedwater system, these CCFs lead to a hazard due to failure of RPV-feeding (plant state b_3) after approx. 5 hours at the earliest.

The simultaneous failure of three nuclear component-cooling-water-system pumps or service-water pumps due to different causes is negligable in contrast to CCFs. The little significance of independent failures compared with CCFs is also valid for other components. CCFs are also dominant in the case of the main-steam-line isolation which can already fail at the failure of two isolation valves.

Nearly 20 % of the result are put down to CCFs with additional independent failures and/or additional failure of planned manual actions.

The diversely designed ARHR-system reduces the contribution of hazard states which can be exclusively put down to CCFs ($4.4 \cdot 10^{-6}$/a) to approx. 40 % of the total frequency. Here, the important factors are the failure of the RPV water-level-measurement devices at a loss of the main feedwater (ATWS) as well as the loss of the 24-V-DC power supply at the loss of preferred power. In contrast to this, the CCFs previously dominating without ARHR now do no more lead exclusively but only in connection with additional, independent failures of components of the ARHR-system to hazard states of the b_1 or b_3 categories.

At the evaluation of the CCF-potential it must be kept in mind that the used data of generic kind as there were no methods available for the determination of plant-specific data. Plant-specific conditions were, however, taken into account at the investigation of the transferability.

The influence of the failure of planned manual actions was determined by using "screening values" for error probabilities. Without considering ARHR and the additional shutdown line, approx. 11 % of the frequencies of hazard states are put down to failure combinations that include a failure of manual actions combined with CCFs, like e.g.:

- no manual feeding into the pressure-suppression pool in connection with a failure to start of the nuclear component-cooling-water pumps, service-water pumps, or residual-heat-removal pumps due to CCF (only significant at loss of main feedwater supply),
- no manual activation of RPV-feeding at CCF of the RPV water-level-measurement devices,
- no activation of the emergency diesels at CCF of the 220-V-DC power supply.

The high grade of automation of the plant contributes greatly to the relatively low contribution of human maloperations.

There are no event sequences which lead to a hazard state due to failure of planned manual actions only.

Table 5-3 Frequencies of plant hazard states for initiating events (disregarding ARHR, disregarding additional shutdown line)

Hazard state			Initiating events and frequencies 1/a									
			Transients					LOCA			ATWS	
plant state		Period of time until hazard state occurs (min)	T1	T2	T3	T3T2	T4	LA1-FD	LI1-FD	LI1-RL	loss of main heat sink, no scram	total of frequencies
			4.0E-2	2.0E-1	5.0E-1	3.0E-1	1.0E-1	2.9E-3	4.3E-3	3.1E-3	1.0E-6	
b_1	LP/HP	600	2E-7	5E-7	2E-5	1.5E-6	3.9E-6	1E-7	ε	ε	ε	**2.6E-5**
b_2	LP/HP	10	n. a.	n. a.	n. a.	n. a.	n. a.	n.a.	n. a.	n. a.	n. a.	n. a.
b_2*	LP	600	n. a.	n. a.	n. a.	n. a.	n. a.	9E-8	n. a.	n. a.	n. a.	**9E-8**
b_3	HP	<15	-	-	-	-	-	-	-	-	1.0E-6	**1.0E-6**
b_3	LP/HP	30	2E-7	4E-7	ε	7E-7	ε	ε	ε	ε	-	**1.3E-6**
b_3 (b_1)	LP	15	-	-	-	-	-	-	4E-7	3E-7	-	**7E-7**
b_3 (b_1)	LP	30	6E-8	9E-7	ε	5E-7	2E-7	ε	ε	ε	-	**1.7E-6**
b_3 (b_1)	LP	300	1.6E-6	3.7E-6	7E-7	1.2E-5	ε	ε	ε	ε	-	**1.8E-5**
b_3 (b_1)	HP	60	1.1E-6	ε	ε	ε	ε	ε	ε	ε	-	**1.1E-6**
total b_3			3.0E-6	5.0E-6	8E-7	1.4E-5	2E-7	ε	4E-7	3E-7	1.0E-6	**2.4E-5**
b_4	HP	10	1E-8	ε	2E-7	9E-8	ε	ε	ε	ε	ε	**3E-7**
total of frequencies			**3.2E-6**	**5.5E-6**	**2.0E-5**	**1.5E-5**	**4.1E-6**	**2E-7**	**4E-7**	**3E-7**	**1.0E-6**	**5.0E-5**
total of mean unavailabilities of system functions:			8.0E-5	2.8E-5	4.1E-5	5.1E-5	4.1E-5	7.0E-5	9.7E-5	9.7E-5	1.0	

ε = (< 10^{-8}/a) ; n. a. = not assessed

Table 5-4 Frequencies of plant hazard states for initiating events (with consideration of ARHR and additional shutdown line)

Hazard state			Initiating events and frequencies 1/a									
			Transients					LOCA			ATWS	
plant state		Period of time until hazard state occurs (min)	T1	T2	T3	T3T2	T4	LA1-FD	LI1-FD	LI1-RL	loss of main heat sink, no scram	total of frequencies
			4.0E-2	2.0E-1	5.0E-1	3.0E-1	1.0E-1	2.9E-3	4.3E-3	3.1E-3	1.0E-6	
b_1	LP/HP	600	ε	2E-8	6E-7	3E-8	1E-7	ε	ε	ε	ε	**7E-7**
b_2	LP/HP	10	n. a.	n. a.	n. ab.	n. a.	n. a.	n. a.	n. a.	n. a.	n. a.	n.a.
b_2*	LP	600	n. a.	n. a.	n. a.	n. a.	n. a.	2E-8	n. a.	n. a.	n. a.	**2E-8**
b_3	HP	<15	-	-	-	-	-	-	-	-	1.0E-6	**1.0E-6**
b_3	LP/HP	30	8E-8	1E-7	4E-8	7E-7	1E-9	ε	ε	ε	-	**9E-7**
b_3 (b_1)	LP	15	-	-	-	-	-	-	8E-9	6E-9	-	**1E-8**
b_3 (b_1)	LP	30	ε	4E-9	ε	ε	ε	ε	ε	ε	-	**4E-9**
b_3 (b_1)	LP	300	5E-8	2E-7	7E-8	2E-7	1E-8	ε	ε	ε	-	**4E-7**
b_3 (b_1)	LP	60	1.2E-6	ε	ε	ε	ε	ε	ε	ε	-	**1.2E-6**
total b_3			1.3E-6	1E-7	1E-7	9E-7	ε	ε	9E-9	6E-9	1.0E-6	**3.4E-6**
b_4	HP	10	1E-8	ε	2E-7	9E-8	ε	ε	ε	ε	ε	**3E-7**
total of frequencies			**1.3E-6**	**1E-7**	**8E-7**	**1.0E-6**	**1E-7**	**2E-8**	**9E-9**	**6E-9**	**1E-6**	**4.4E-6**
total of mean unavailabilites of system functions:			3.3E-5	7E-7	1.6E-6	3.4E-6	1.3E-6	6.5E-6	2E-6	2E-6	1.0	

ε = (< 10^{-9}/a); n. a. = not assessed

TRANSIENTS

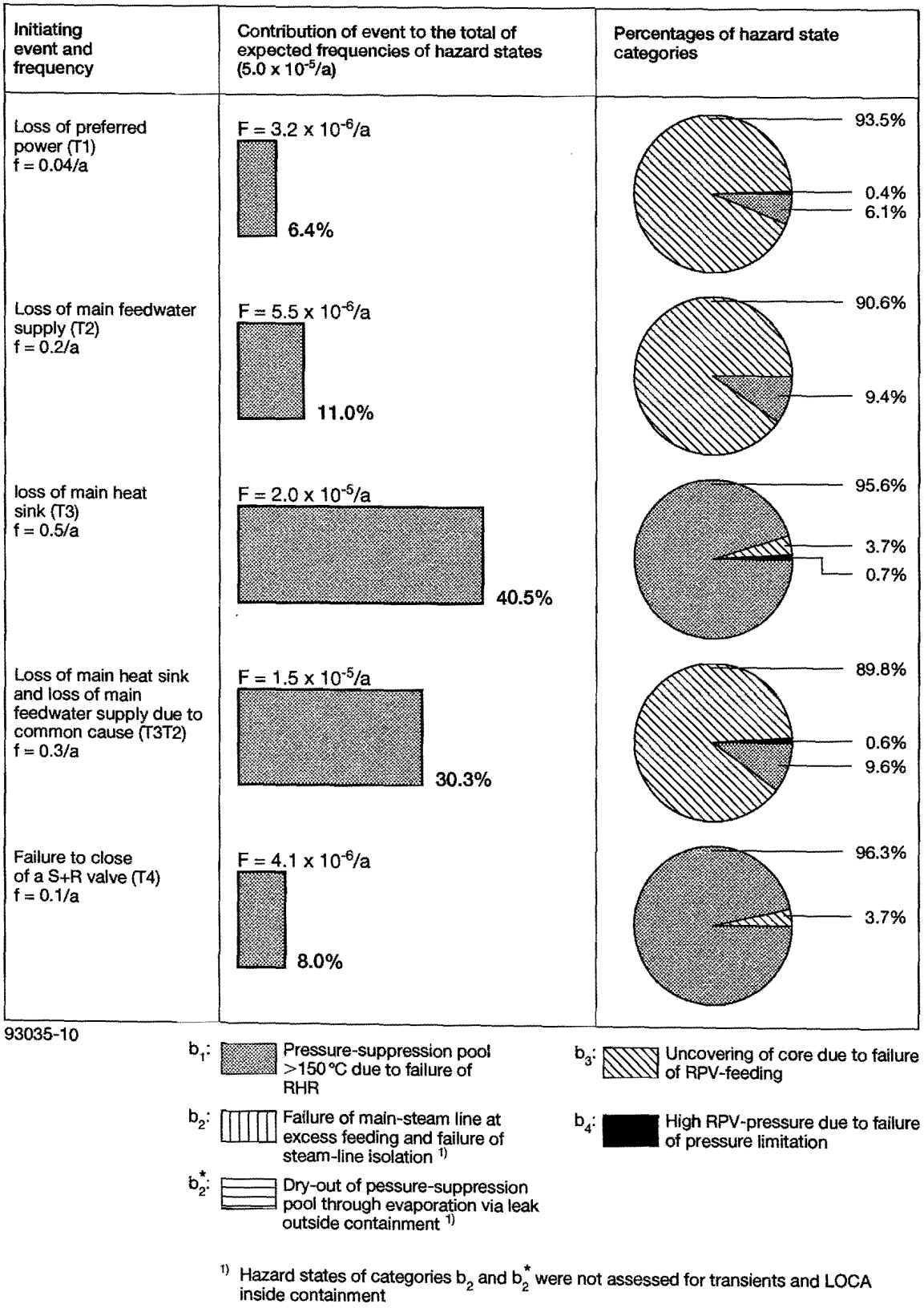


Figure 5-1 Transients; contributions to the total of the expected frequencies of hazard states (without ARHR, without modified shutdown line)

LOSS-OF-COOLANT ACCIDENTS

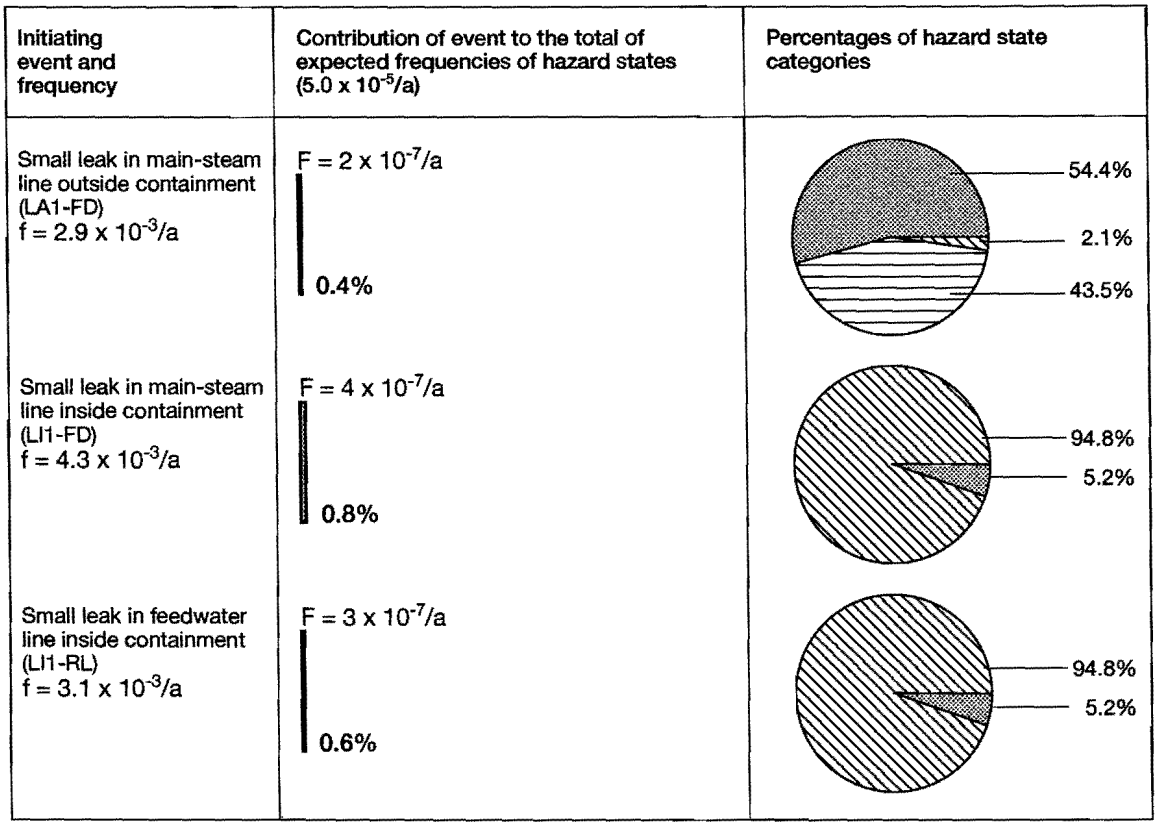
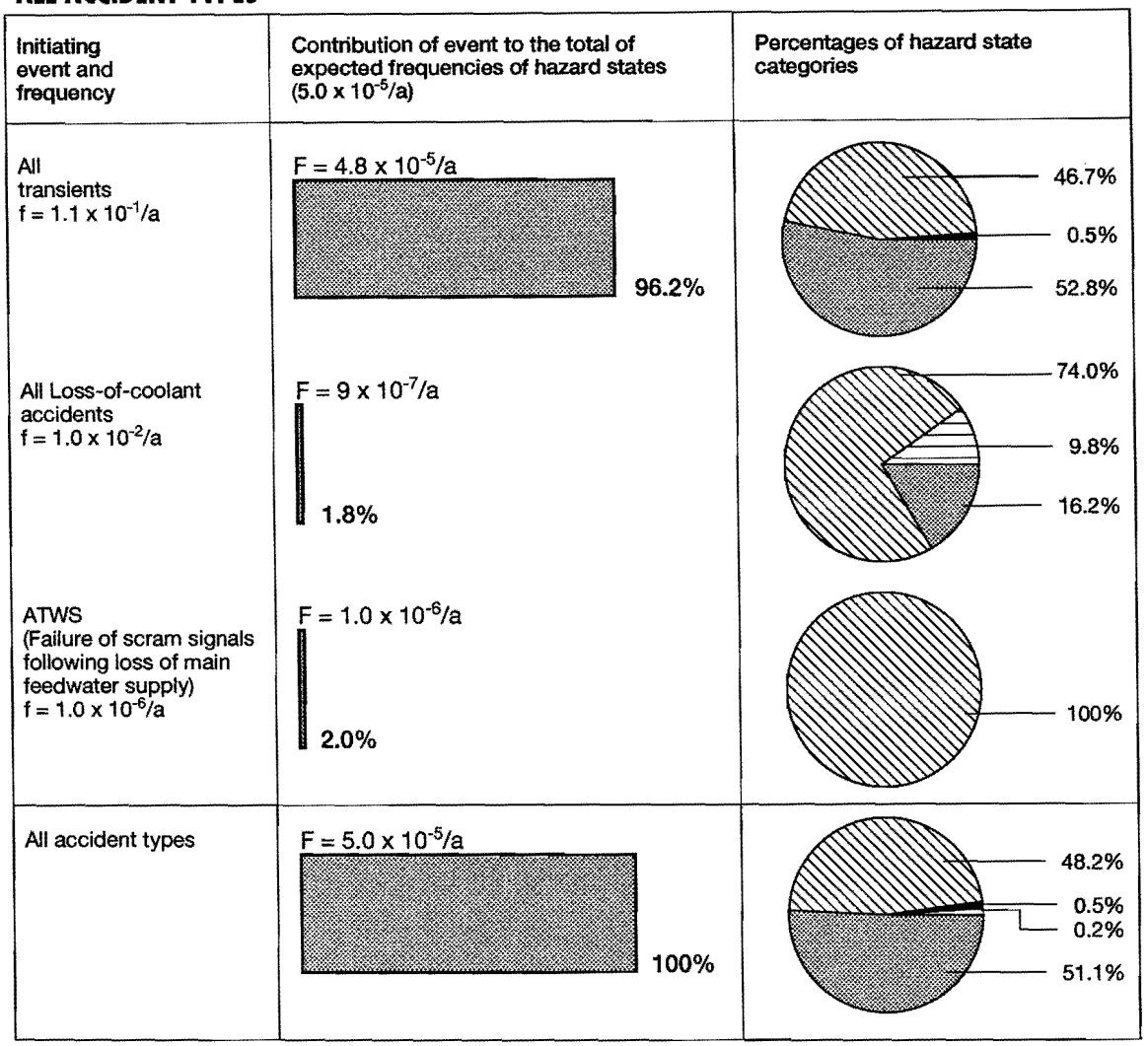


Figure 5-2 Loss-of-coolant accidents; contributions to the total of the expected frequencies of hazard states (without ARHR, without modified shutdown line)

ALL ACCIDENT TYPES



1) Hazard states of categories b_2 and b_2^* were not assessed for transients and LOCA inside containment

Figure 5-3 Plant-internal initiating events; contributions to the total of the expected frequencies of hazard states (without ARHR, without modified shutdown line)

TRANSIENTS

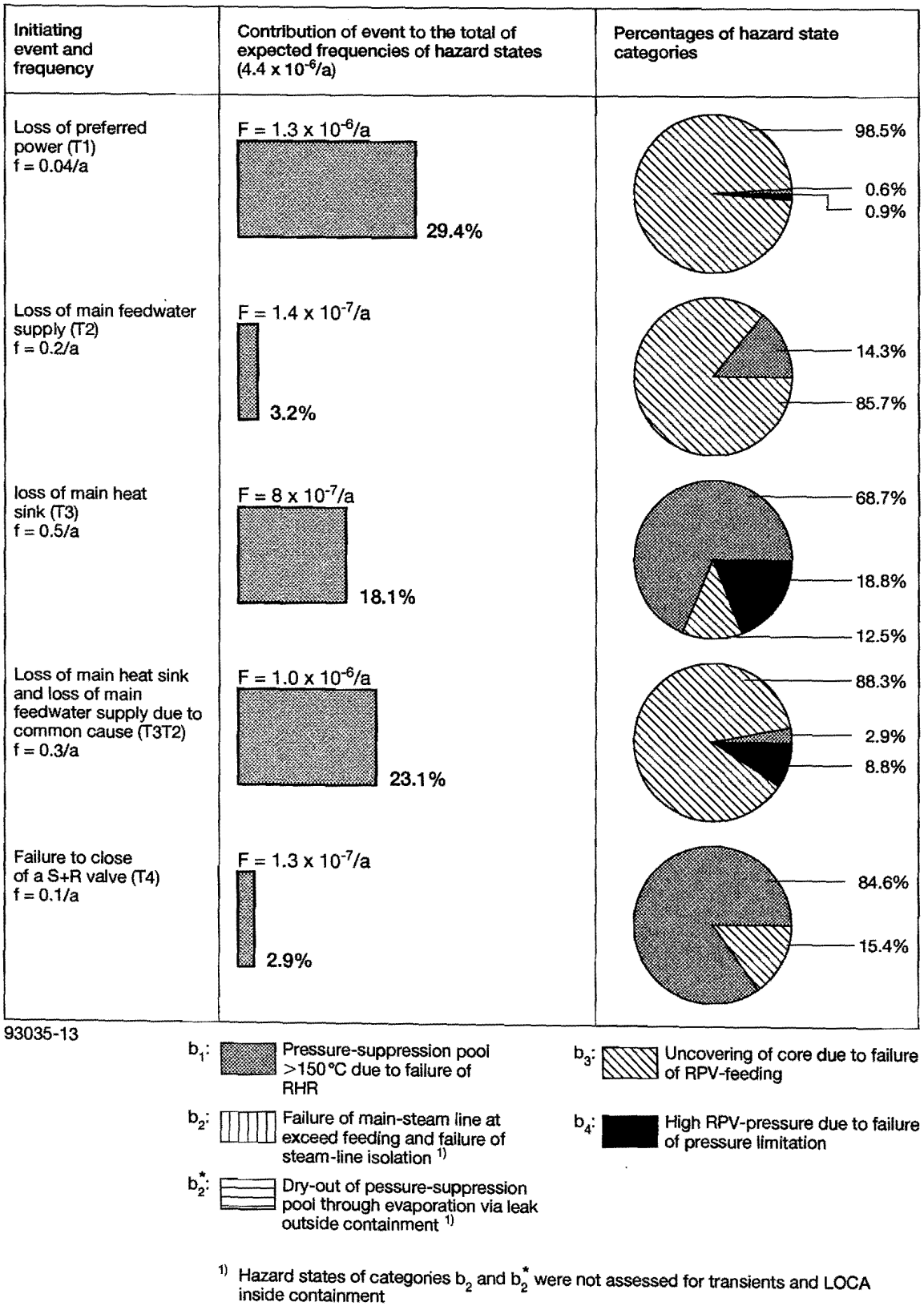
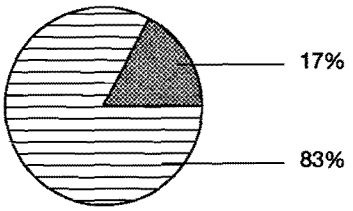
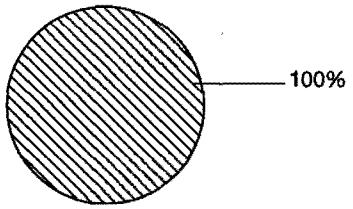
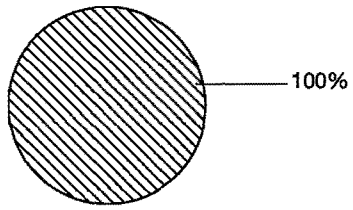


Figure 5-4 Transients; contributions to the total of the expected frequencies of hazard states (with ARHR, with modified shutdown line)

LOSS-OF-COOLANT ACCIDENTS

Initiating event and frequency	Contribution of event to the total of expected frequencies of hazard states (4.4×10^{-6}/a)	Percentages of hazard state categories
Small leak in main-steam line outside containment (LA1-FD) $f = 2.9 \times 10^{-3}$/a	$H = 2 \times 10^{-8}$/a 0.4%	
Small leak in main-steam line inside containment (LI1-FD) $f = 4.3 \times 10^{-3}$/a	$H = 9 \times 10^{-9}$/a 0.2%	
Small leak in feedwater line inside containment (LI1-RL) $f = 3.1 \times 10^{-3}$/a	$H = 6 \times 10^{-9}$/a 0.1%	

93035-14

b_1: Pressure-suppression pool >150 °C due to failure of RHR

b_2: Failure of main-steam line at excess feeding and failure of steam-line isolation [1)]

b_2^*: Dry-out of pessure-suppression pool through evaporation via leak outside containment [1)]

b_3: Uncovering of core due to failure of RPV-feeding

b_4: High RPV-pressure due to failure of pressure limitation

[1)] Hazard states of categories b_2 and b_2^* were not assessed for transients and LOCA inside containment

Figure 5-5 Loss-of-coolant accidents; contributions to the total of the expected frequencies of hazard states (with ARHR, with modified shutdown line)

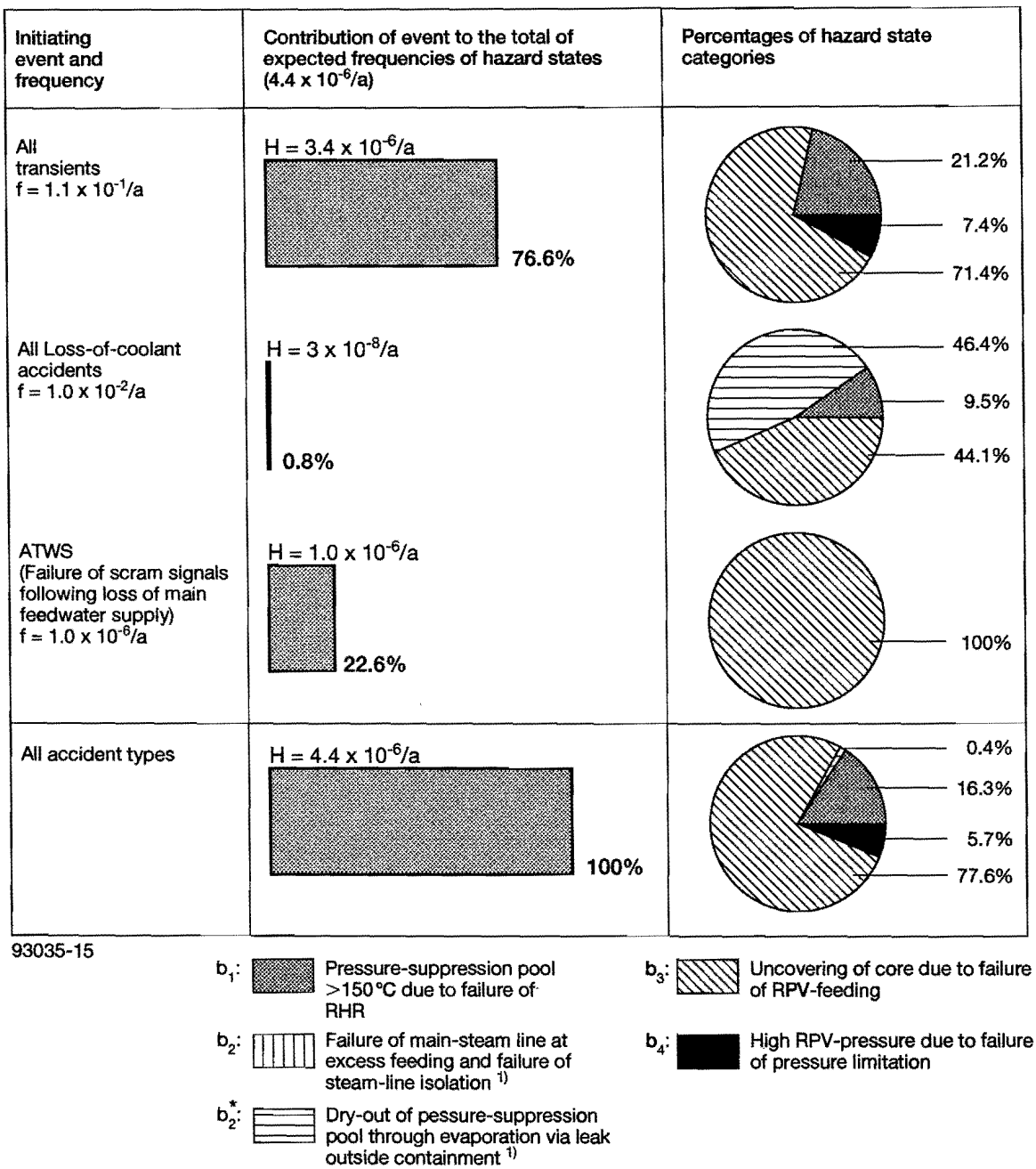


Figure 5-6 Plant-internal initiating events; contributions to the total of the expected frequencies of hazard states (with ARHR, with modified shutdown line)

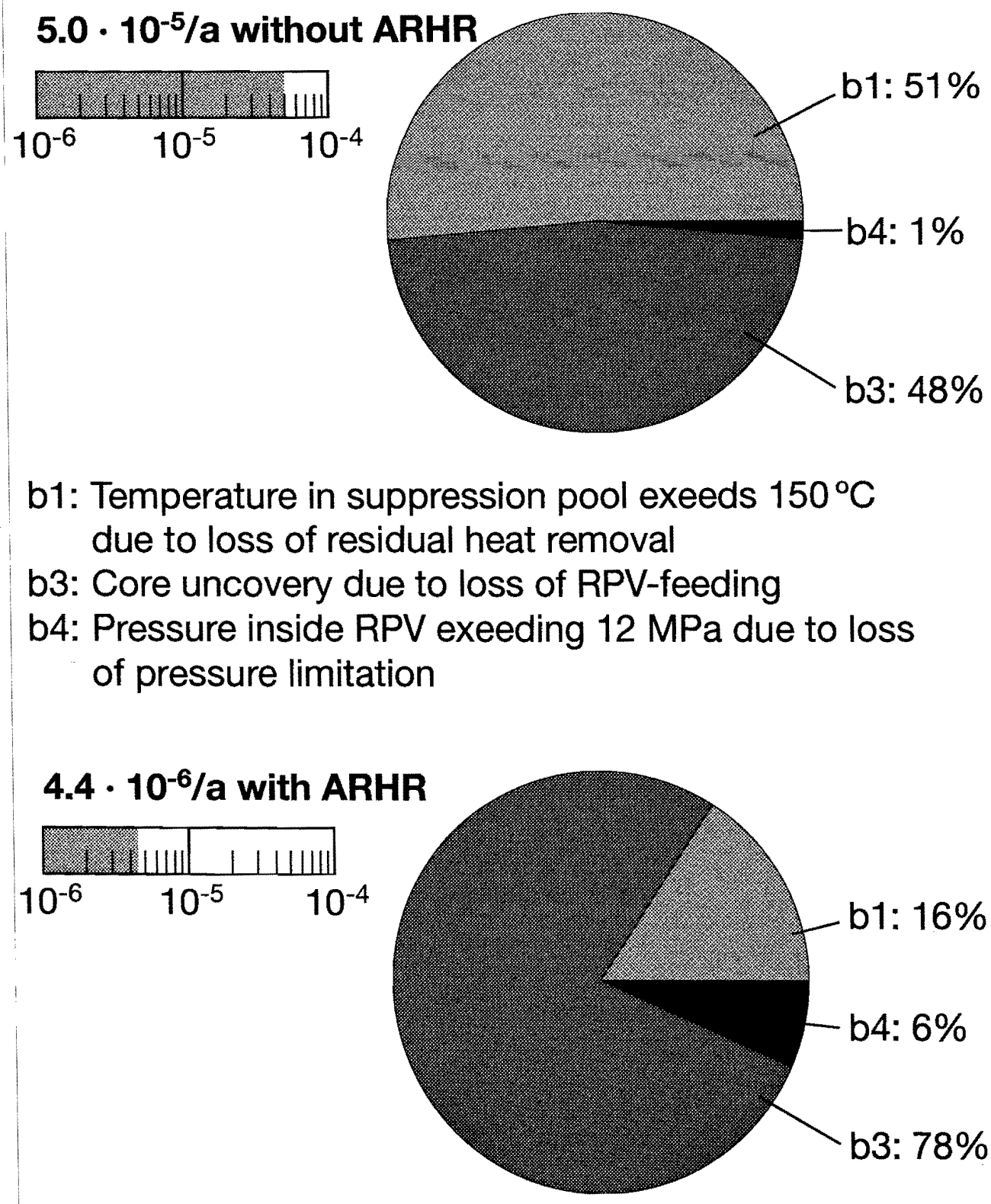


Figure 5-7 Frequencies of hazard states and contributions to plant states with and without consideration of ARHR.

6 Accident-Management Measures

Accident-management (AM) measures comprise all measures which can be taken inside the plant for the early and clear detection of beyond-design-basis events, for controlling them and bringing them to an end with the least serious consequences possible. A basic prerequisite is the flexible use of the safety and operational systems, if necessary also outside the scope of application intended at their design, and the use of external systems.

In a large number of event sequences, hazard states can be controlled by preventive AM-measures, and damage states can be avoided. If the failure of such measures results in a damage state there are still mitigating AM-measures which can be carried out.

Preventive AM-measures are initiated if following the failure of system functions certain predicted plant states are reached. These measures are usually laid down in the accident-management manual.

The measures serve for maintaining or re-establishing

- sub-criticality
- RPV-feeding at high pressure, e.g. re-activation of the main feedwater-supply system
- RPV-feeding at low pressure, e.g. feeding with mobile pumps
- heat removal
- retention of activity and integrity of the containment, e.g. by containment venting
- power supply.

6.1 Possibilities of Prevention of Damage States through Accident-Management Measures

Examples of AM-measures and their potential to prevent damage states are discussed in the following for typical plant states.

- **Temperature in the pressure-suppression pool exceeds 150 °C due to failure of residual-heat removal (b_1)**

Insufficient residual-heat removal leads to a temperature increase of the water in the pressure-suppression pool and, after set temperature thresholds have been exceeded, to a failure of RPV-feeding. When the water in the pressure-suppression pool heats up and partially evaporates, the temperature and the pressure inside the containment increase, which endangers the containment's integrity. The temperature of the water in the pressure-suppression pool reaches 150 °C after 10 hours at the earliest.

Before this state is reached, residual-heat removal can be re-established by bringing back into operation RHR-systems that have previously failed. If this cannot be achieved, the residual heat has to be removed by containment venting. In this case the integrity of the containment can be maintained.

This measure is to be initiated at a containment pressure of p_{Cont} = 0.3 MPa. The system is designed in such a way that about 1 % of thermal power (approx. 40 MW) can be removed from the containment at a containment pressure of p_{Cont} = 0.6 MPa.

RPV-feeding with the pumps of the RHR-system fails when the temperature of the water in the pressure-suppression pool reaches 150 °C. RPV-feeding can then only be carried out with the main feedwater system, independent of the temperature of the water in the pressure-suppression pool. If this system also fails there still are possible measures available which are provided for the failure of RPV-feeding (b_3).

- **At failure of steam-line isolation and continuing RPV-feeding, the RPV water level exceeds the level of the steam lines, involving subsequent failure of the steam line or the connecting systems (b_2)**

Excess feeding of the steam line outside the containment can occur either at "RPV-flooding" and failure of steam-line isolation or at "keeping RPV water level" with the failure to shut off RPV-feeding and failure of steam-line isolation. After feeding has been interrupted and steam-line isolation has been re-established manually, residual-heat removal has to be secured. If all measures provided for the re-establishment of steam-line isolation have failed, the residual heat can still be removed from the RPV via the modified shutdown line. In case this measure should also prove ineffective, there still remain other possibilities of injection into the RPV for maintaining core cooling.

- **The normal water level in the pressure-suppression pool falls below 6.5 m due to a leak in a steam line outside the containment and failure of the steam-line isolation with subsequent partial evaporation of the coolant (b_2*)**

Steam-line isolation has to be re-established through manual actions. If these measures fail, residual-heat removal from the RPV can be secured via the modified shutdown line.

- **RPV water level reaches the bottom of the core due to failure of RPV-feeding (b_3)**

At a failure of RPV-feeding there are several measures available for coolant injection. The injections which become effective automatically (RM/RL direct link, draining of feedwater tank) lead to a prolonging of the time until the onset of a hazard. In the evaluation of the injection possibilities it must be considered that some measures do not provide for lasting injection due to the limited amount of water available.

If after a failure of the injection systems AM-measures using pumps with low pumping capacity become necessary, RPV-pressure must first be reduced. This, however, always goes along with a loss of coolant from the RPV. It still has to be investigated under which consequences the measures available at that stage (e.g. fire-fighting

system, mobile pumps, injection of service water via an RHR-tie) can still become effective in time.

6.2 Evaluation of Accident-Management Measures in other Probabilistic Safety Analyses

The success probabilities of the described AM-measures are not assessed in the analysis as comprehensive investigations into the feasibility and the effectiveness of these measures still need to be performed.

AM-measures are assessed in an number of studies. It must, however, be noted that it is common practice abroad to include AM-measures in procedure packages which do not distinguish between measures according to operating manual and accident-management manual as it is the case in Germany. An extensive basis for the assessment of operator actions can be found in the French studies EPS 900 and EPS 1300, albeit for pressurised water reactors. Here, the basis is formed by comprehensive simulator experiments performed by Electricité de France (EdF). For some selected cases the assessment is carried out by directly using the statistics drawn up from the simulator experiments. For those cases where the simulator experiments could not be directly applied, the assessment was made on the basis of the statistics with consideration of adaptability criteria. The determined probabilities result from the probabilities for successful diagnoses under different framework conditions and for the success of the actions to be performed, also under different framework conditions.

Table 6-1 contains a presentation of the data of the French studies relating to the failure probabilities at two different degrees of difficulty of diagnosis and execution and for various grace periods.

The failure probabilities refer to cases in which "a measure" can be performed "with an available system" which has the capacity to take over the duties of a function that has failed. There are lower failure probabilities if several measures are available that can be carried out with the help of several systems of which each has the capacity to take over the function of the system that has failed.

Table 6-1 Failure probabilities (p_{OP}) for operator actions at AM-measures according to EdF simulator experiments

Degree of difficulty of diagnosis and execution	Time span in minutes from reaching initiation criteria for AM measures until the onset of the hazard state or damage state (grace period)				
	$t \leq 20$	$20 < t < 30$	$30 < t \leq 60$	$60 < t \leq 200$	$t > 200$
low	$1^* > p_{OP} > 0.04$	$0.04 \geq p_{OP} \geq 0.02$	$0.02 \geq p_{OP} \geq 0.01$	$0.02 \geq p_{OP} \geq 0.01$	$0.02 \geq p_{OP} \geq 0.01$
average	1	$1 \geq p_{OP} > 0.1$	$0.1 \geq p_{OP} > 0.06$	$0.06 \geq p_{OP} > 0.04$	$0.04 > p_{OP} > 0.02$
high	1	$1 \geq p_{OP} > 0.2$	$0.2 \geq p_{OP} > 0.08$	$0.08 \geq p_{OP} > 0.06$	$0.06 \geq p_{OP} > 0.04$

* $p_{OP} = 1$ for $t < 7$

The given values only indicate the failure probabilities for diagnosis and actions to carry out the AM-measures. In addition to this there are the failure probabilities p_A of the required systems.The total failure probabilities consequently result in:

$$p_{AM} = p_{OP} + p_A - p_{OP}p_A.$$

American studies (NUREG-1150) /3/ of the LWR-plants at Surry, Sequoyah and Peach Bottom also assess the failure probabilities for operator actions, albeit not as classified in such detail as in EPS 900 /4/ and EPS 1300. They lie between 0.01 for simple situations and 0.5 for complex situations.

The assessment of failure probabilities of AM-measures in published PSAs leads integrally to the results shown below in Table 6-2. This assessment includes in part measures which are carried out in German plants as part of the instructions of the operating manual. This is why in most cases there is a numerically higher rate of effectiveness of the AM-measures than in the German Risk Study, Phase B (DRS-B) /1/.

Table 6-2 Integral assessment of AM-measures in different studies

Frequency of core meltdown with AM-measures / Frequency of core meltdown without AM-measures					
Surry /3/	Sequoyah /3/	Peach Bottom /3/	EPS 900 /4/	Japan 1100 MWe /5/	Biblis B 1300 MWe /1/
PWR	PWR	BWR	PWR	PWR	PWR
1/23 (0.043)	1/4.7 (0.21)	1/50 (0.02)	1/18 (0.055)	1/26 (0.038)	1/7.5 (0.13)

6.3 Summary and Outlook

The values indicated in Table 6-1 cannot be implicitly transferred to the reference plant of the BWR safety analysis. They may, however serve for orientation purposes in order to estimate the prospects of success of AM-measures for some typical cases. The decisive factors in this context are the two parameters of the grace period and the number of the measures that are feasible and those that are to be carried out.

- Temperature in the pressure-suppression pool exceeds 150 °C due to failure of residual-heat removal (b_1).

  The determined frequency of hazard states where plant state b_1 is dominant is 2.6 · 10^{-5}/a without ARHR. For controlling the hazard state or for preventing a damage state, the measure of containment venting and a measure for RPV-feeding must be carried out. The grace period for this is at least 8 hours.

- At failure of steam-line isolation and continuing RPV-feeding, the RPV water level exceeds the level of the steam lines, involving subsequent failure of the steam line or the connecting systems (b_2).

  The frequency of hazard states where plant state b_2 is dominant was not determined. For controlling the hazard state or for preventing a damage state, RPV-feeding must be interrupted manually. There are approx. 30 minutes available for this. If steam-line isolation can be re-established by manual actions, residual-heat removal via the pressure-suppression pool is to be secured. There are approx. 100 minutes available for this as from the interruption of RPV-feeding. If steam-line isolation cannot be re-established, residual-heat removal from the RPV must be secured within these 100 minutes by using the modified shutdown line.

- The normal water level in the pressure-suppression pool falls below 6.5 m due to a leak in a main-steam line outside the containment and failure of the steam-line isolation with consequent partial evaporation of the coolant (b_2*)

For controlling the hazard state or for preventing a damage state, the manual actions for re-establishing steam-line isolation or the measures for shutting the plant down via the shutdown line must be carried out. The grace period for this is at least 2 days.

- RPV water level falls below the bottom of the core due to failure of RPV-feeding (b_3).

  The frequency of hazard states where measures must be carried out within 30 to 60 minutes for controlling them or for preventing a damage state is $4.3 \cdot 10^{-6}$/a without ARHR. Due to the short time span and the more difficult conditions at the diagnosis (total failure of RPV water-level-measurement device), only few success probabilities are to be expected in these cases for the execution of AM-measures. This also applies to the case of loss of preferred power with the total failure of DC-power supply ($1.1 \cdot 10^{-6}$/a), in which there is 1 hour available and which is marked by high pressure in the RPV.

  The determined frequency of hazard states which lead to plant state b_3 as a consequence of insufficient heat removal is $1.9 \cdot 10^{-5}$/a without ARHR. For controlling the hazard state or for preventing a damage state, the measures for RPV-feeding and those which are necessary for preventing plant state b_3 must be carried out. The grace period here is more than 200 minutes.

- RPV-pressure exceeds design pressure (approx. 12 MPa) by a factor of 1.3 following failure of pressure limitation of the reactor cooling system (b_4).

  The determined frequency of hazard states where plant state b_4 is dominant is $3 \cdot 10^{-7}$/a without ARHR. The time span during which measures for the prevention of damage states must be carried out is approx. 10 minutes. For this reason no AM-measures are considered for this case.

The investigations show that in approx. 90 % of the total frequencies of hazard states there exist long grace periods and several possibilities for carrying out AM-measures, i.e. favourable conditions for their successful execution. In approx. 10 % of all frequencies of hazard states with short grace periods, only low success probabilities

are to be expected for the execution of AM-measures. If investigation results from other plants are used for an orientating estimate of the success probabilities, the result without consideration of the ARHR-system for the total frequencies of damage states resulting from plant-internal events lies at $< 10^{-5}$/a.

Further, more detailed investigations of the effectiveness and feasibility of the measures under consideration of the special conditions of the reference plant are necessary for a corroborated quantification of the AM-measures.

7 Common-Cause Initiators (CCI)

This chapter discusses events whose impact can affect large parts of the plant by spreading over redundancies and different systems. Such events either lead to a mechanical and/or thermic load acting on structures, components and systems or to the flooding of whole areas of the plant.

The causes and the impacts of the events on the plant are described and the event frequencies are determined. A differntiation will be made in this context between "plant-internal common-cause initiators" like fire and flooding and "plant-external common-cause initiators" like earthquake and airplane crash.

Detailed investigations were carried out for the events of flooding, fire and earthquake. For the remaining events of airplane crash, flooding due to high tide, explosion blast wave and impacts from the neighbouring unit, no relevant contributions are to be expected for the frequencies of hazard and damage states.

7.1 Flooding

Plant-internal floodings can trigger off transients where the systems necessary for controlling the accident may be restricted in their functioning.

Flooding situations caused by the failure of systems containing water (e.g. pipe break) are investigated for the reference plant in the following buildings: reactor building, auxiliary building, nuclear operating building, turbine building, switch-gear building, emergency-diesel building, emergency-diesel and refrigeration-plant building, service-water-pump building.

In the reactor building, the areas of the individual partial systems (redundancies) as well as the scram area are physically separated by constructional elements up to the level of $\pm$ 0.00 m (i.e. 8.30 m above the bottom raft) so that in the case of flooding no water below this level can flow over from one redundancy to the neighbouring redundancy or into the scram area.

Whether the flooding of buildings or partial areas of buildings leads to safety-relevant impacts on the entire plant depends upon the possible amount of leaks, the rooms

concerned, the safety installations installed in these rooms, the detection possibilities and the possible counter-measures taken by the operating personnel.

The investigations show that only one leak in the nuclear service-water system (VE) is sufficient to cause extensive flooding in the reactor building due to the large amount of water pumped on by the service-water pump (approx. 3500 m^3/h) and the unlimited amount of water available (Danube water).

Only two trains of the three-train nuclear service-water system lead into the corresponding redundancies of the annulus. One train leads into the nuclear operating building and thus cannot flood the annulus. Leaks in the two former trains can be detected by signals from the building-drainage system, the leak-detection system and the water-level measurement in the respective residual-heat-removal chambers.

Thereby the automatic shutdown of the service-water pump, the service-water system as well as of the LP and HP-pumps of the RHR-system and the automatic isolation of the pipes leading through the water in the pressure-suppression pool is initiated. The flooding consequently remains restricted to the affected area of a partial system.

At failure of the above-mentined measures the affected area would, e.g. at a break of the service-water line, be flooded after approx. 20 minutes due to the large amount of water pumped on by the service-water pump; this would result in water flowing over into the area of neighbouring partial systems and/or into the scram area. The frequency of such events as well as the frequency of hazard states are estimated to be $< 10^{-7}/a$, taking into account the plant-specific conditions.

Flooding of the auxiliary building, nuclear operating building, turbine building, switch-gear building, emergency-diesel building, emergency-diesel and refrigeration-plant building and the service-water-pump building has no safety relevance due to the implemented constructional and system-technological measures.

7.2 Fire

The main inflammable materials are cable-isolation materials and various types of oil for the lubrification of technical components of machinery. Both materials exist in

various amounts in different locations. The following buildings or partial building areas of the reference plant were investigated:

- reactor building with
  - containment interior
  - rooms outside the containment
- switch-gear building
- emergency-diesel building
- turbine building
- nuclear operating building
- auxiliary building
- building for safety-relevant service-water supply

- **Possible fire scenarios inside the containment and their frequencies**

The investigations show that fires are only safety-relevant inside the containment. There are no constructional sub-divisions for fire protection inside the containment apart from cable ducts in the sump area. The main inflammable materials are cable isolations (approx. 8000 kg), of which approx. 20 % are located inside the control-rod-drive chamber, and lubricants in the case of a leakage in the oil supply of the coolant pumps. Thus the events of cable fire and oil fire with an induced cable fire were investigated.

Due to an insufficient database for German plants it is necessary to fall back on generic data from American operating experience for determining the frequency for cable fires. According to those figures, the frequency of cable fires inside the containment is estimated at $3 \cdot 10^{-3}$/a.

By using generic data, the frequency of an oil leakage (leak rate higher than 10 kg/h up to 150 kg/h) of which it is assumed that it is not detected until there is a relevant amount of oil is estimated at 10^{-3}/a. Larger leakage amounts do not constitute a relevant initiating event due to the lower frequency of large leaks and the fact that they are more easily detectable and consequently can be isolated more quickly. The

investigations show that potential ignition mechanisms like ignition through contact with hot plant components, auto-oxidation in isolation materials or ignition through contact with electrical equipment were not found in areas of possible leakage or areas where oil has collected; however, they cannot be totally excluded. Therefore, for quantifying the frequency of oils fires, the conditional ignition probability is estimated at lower than 10^{-2}. There presently is no methodological approach for obtaining a more precise plant-specific estimate.

A combined oil/cable fire has greater relevance than a cable fire due to the faster temperature and pressure increase in the containment. According to the investigations, there are temperatures from about 400 °C at the beginning in the lower drywell of the containment. With the development of the cable fire they reach short-term levels of about 1200 °C in the fire area; even in the physically more distant upper area of the containment they still exceed 700 °C for a short while. Fire-fighting measures were not taken into consideration for these calculations. Such a fire would be extinguished after approx. 20 to 30 minutes due to the lack of oxygen.

The same high temperatures as in the case of an oil/cable fire can occur at a cable fire alone when no fire-fighting measures are carried out. Assuming a local cable ignition, the speed of the fire spreading and therefore also the temperature increase are presumably considerably lower; thus the effect of fire-fighting measures can be assessed to be more favourable.

- **Effects on structures, components and structural elements**

Using the temperature and pressure developments determined for a combined oil/cable fire in certain containment areas, the following effects are more closely investigated:

- stability of structural elements and of the RPV as well as integrity of the confinement systems carrying coolant
- functions of components of machinery, e.g. gauges and instruments
- failure of cables due to high temperature or combustion
- behaviour of instrumentation

- pressure build-up inside the containment.

The investigations have shown that the stability of structural elements and of the RPV as well as the integrity of the confinement systems carrying coolant and of the control rod drive pipes are not put at risk. The integrity of the containment under consideration of thermal loads was not investigated.

Components of machinery can be affected to varying degrees. It can be assumed that there is neither an effect on the penetration valves of the main-steam lines lying in the upper part of the containment nor on the check valves of the main feedwater system or the safety and relief valves due to the automatic, spring-actuated operation of these valves. The actuation of these valves via magnetically actuated pilot valves could, however, be put at risk if there is a thermal failure of cables.

According to the analyses, there will be temperatures in all areas exceeding the assumed failure temperature (200 °C) of the cables. Therefore the failure of all electrical instruments may possibly be expected. An exception is the neutron-flux monitoring for the surveillance of the plant state after reactor scram because fire-protection measures have been implemented in an instrument well. Due to thermal loads the RPV water-level-measurement device may also indicate water levels higher than the actually existing level. The calculated results show that there is a sufficient discrepancy between the fire-related pressure increase in the containment and the design value.

- **Plant behaviour at fire inside the containment; assessment**

In the case of a fire inside the containment it is highly probable that reactor scram will be manually activated by the operating personnel following the signal of the very reliable fire-detection system. If this is not the case it can be assumed that automatic measures of the reactor-protection system will be activated (LOCA-signal), especially through the fire-related pressure increase in the containment.

The functions of the process-engineered and electro-technical components of the RHR-system for RPV-feeding and residual-heat removal installed outside the containment are not directly affected by a fire. Inside the containment, however, design limits for the detection of measured data may be exceeded due to the fire; the

possible resulting effects on their availability were not investigated. In the case of an activation of feeding, caused by a pressure increase in the containment (P10-signal), depressurisation is immediately activated alongside steam-line isolation. A failure of feeding caused by too high RPV pressure is highly unlikely because the failure of the magnet pilot valves of the S&R valves caused by failure of cables due to high temperatures will occur later than the initiation of depressurisation through the LOCA-signal (P10-signal) and because pressure limitation through the spring-actuated pilot valves is very unlikely to be put at risk.

The determination of the frequencies of fire-related hazard states carries large uncertainties.The investigations resulted in frequencies for cable fires of $3 \cdot 10^{-3}$/a and for oil fires of $< 10^{-5}$/a, with a conditional ignition probability of $< 10^{-2}$ being used. For the failure probabilities of fire-fighting measures, ranges were estimated of 1 to 0.1 for oil fires and of $< 10^{-2}$ for cable fires. Where fire-fighting measures fail, reactor-protection measures are initiated in the case of oil/cabel fires due to the fire-related pressure increase in the containment. Initially, automatic pressure suppression will set in; in the further course of events there will be a pressure increase due to the fire-induced failure of the pressure-limitation function. Such a sequence is controlled if pressure limitation is functioning and RPV-feeding at high pressure is safeguarded.

Event sequences and the boundary conditions for their control can only be determined with difficulty and quantified with great uncertainties due to the various failure probabilities of the electrical instrumentation inside the containment. The frequency of hazard states is generally estimated at well below 10^{-6}/a. In the framework of a balanced safety concept there is therefore no need for any further fire-protection measures.

In connection with the avoidance of H_2-burn due to severe core damage, inerting the containment is discussed as a possible measure. Such a measure would also effectively prevent fires in the containment during power operation. Containment inerting has already been realised in all German nuclear power plants of the BWR line 69 and in foreign plants with a comparable containment.

7.3 Earthquake

The vibrations of the ground caused by an earthquake transmit themselves through the soil to the building structures of a nuclear power plant. Through the earthquake, the building structures are activated to vibrate in accordance with their dynamic behaviour. These building-structure vibrations are transferred to the interior components and parts of the plant. The safety-relevant components and parts of the reference plant are designed to withstand such dynamic loads caused by an earthquake.

The individual steps in determining the earthquake-related risk to building structures and components of the reference plant are as follows:

- determination of realistic seismic load assumptions
  - intensity-dependent site-specific seismic data
    (e.g. maximum acceleration, response spectra of ground accellerations)
  - site-specific frequencies for earthquake intensities
- dynamic building-structure calculations
  - linear-elastic analyses of the stability of building structures
  - determination of intensity-dependent floor-response spectra as earthquake exitation of components
  - estimation of frequencies for the exceeding of design-limit values
- dynamic component calculations
  - linear-elastic analyses of the stability and integrity of mechanical components of machinery
  - evaluation of functional safety
  - estimation of frequencies for the exceeding of design-limit values.

- **Seismic load assumptions**

A focus of the investigations was on the determination of realistic seismic load assumptions on the site of the reference plant. For describing the intensity of the earthquake the macro-seismic intensity I (according to the Medvedev-Sponheuer-Karnik (MSK) scale) was used which is directly connected with loads acting on building structures and with damage. The seismic data necessary for the dynamic calculations - especially free-field response spectra and duration of strong earthquakes - was determined with regard to their intensity. Three intensity grades were considered which according to the experience gathered so far cover the earthquake risk at the site of the reference plant:

$I_1 = 6$ (according to operating-basis earthquake (OBE))
$I_2 = 7$ (according to safe-shutdown earthquake; cf. KTA 2201)
$I_3 = 8$

The free-field response spectra and data on the duration of strong earthquakes were obtained by statistical evaluation of duration measurements of earthquakes at sites with similar ground conditions. The median values (50%-fractiles) of the free-field response spectra that are allocated to the individual intensity states were used as load assumptions at the site. The duration of a strong earthquake depends relatively little on the intensity and was estimated for the present study to be 4 seconds.

The frequency of earthquakes which exceed intensity I at the site was determined with probabilistic methods and geo-seismic models for the site and its further surroundings. Included in these seismicity models are empirically known correlations between the following stochastic quantities: wave energy released at the epicentre (magnitude), distance of the epicentre from the site, energy at the site (intensity). By numerical simulation (Monte-Carlo-method) of a large number of energy-release events at potential epicentres (e.g. faults in the underground layers), such models can determine the frequency of a certain intensity at the site.

The most important results are the exceeding-value rates for the three macro-seismic intensity steps with:

$3 \cdot 10^{-4}$/a	for	I = 6
$3 \cdot 10^{-6}$/a	for	I = 7
$4 \cdot 10^{-8}$/a	for	I = 8.

Ranges of the relevant macro-seismic data - distance from epicentre R and magnitude M - are given along with the intensities.

- **Behaviour of building structures**

Dynamic analyses for the following building structures of the reference plant were carried out, based on site-specific seismic load assumptions:

- reactor building
- emergency-diesel building
- nuclear operating building and auxiliary-plant building
- turbine building.

The analyses served for the verification of the stability of the building structures and for the determination of earthquake excitations at support positions of components.

The linear-elastic analyses that were carried out led to the result that the stability of the investigated buildings is maintained for the following earthquake intensities I:

- reactor building	I = 8
- emergency-diesel building	I = 8
- nuclear operating building and auxiliary-plant building	I = 6
- turbine building	I = 7.

Further investigations for the nuclear operating building and auxiliary-plant building proved that the overall stability of these buildings can still withstand earthquakes with intensities of I = 7 and I = 8.

Under consideration of the contributions of the various earthquake intensities and of the variation of the earthquake acceleration (coefficient of variance of 60%), the

following frequencies were determined for cases where the design-limit values for the buildings are exceeded:

- reactor building $6 \cdot 10^{-7}$/a
- emergency-diesel building $6 \cdot 10^{-7}$/a
- nuclear operating building and auxiliary-plant building $6 \cdot 10^{-7}$/a
- turbine building $6.3 \cdot 10^{-5}$/a.

The limit values in the building structures correspond to the "permissible loads" used in the design calculations.

A first simplified evaluation of the stability of the turbine building led to the conclusion that the building is safely designed in a deterministic way for an intensity I = 6 connected with a probability of exceedance of seismic design limits with a frequency of $2.4 \cdot 10^{-3}$/a. The relevant limit value in this preliminary investigation was the yield limit of the bearing construction of the roof trusses in a linear-elastic analysis.

A more detailed study of the bearing behaviour of the roof construction yielded the conclusion that the roof trusses are not the weakest link because the roof panel itself is connected directly to the gable and side walls. Horizontal forces acting in the roof panel can hence be transmitted to these surrounding structures. From the resulting reserves in load-bearing capacity it was deduced with consideration of site-specific linear earthquake-spectra that the stability of the turbine building is assured deterministically also for an intensity I = 7. The corresponding design limits for seismic loading are exceeded with a computed frequency of $6.3 \cdot 10^{-5}$/a to which the main part is contributed, as in the case stated above, by the intensity I = 6. The frequency value determined on this basis is taken as an upper estimated value for the probability of leaks in the steam lines due to a collapse of the roof construction. Non-linear plastic analyses would be required for an even more precise determination of the failure probability.

- **Component behaviour**

The stability of the heat exchangers of the TF-system and the scram accumulator tanks in the reactor building at seismic impact was investigated due to the

safety-relevance of these components. The relevant accelerations at the anchoring points of the components were determined within the framework of the preceding investigations of the reactor building for an earthquake intensity of I = 8.

The performed analyses have shown that the stability of the investigated components is safeguarded for the earthquake intensity I = 8.

In a procedure analogous to the ones used with the buildings (see above), the following frequencies for cases where limit values are exceeded (yield limit, displacement limit values) due to an earthquake were determined for the investigated components:

- heat exchangers (TF) $2 \cdot 10^{-7}$/a
- scram accumulator tank (YT) $2 \cdot 10^{-7}$/a.

The indicated values, particularly the one for the heat exchangers, are to be assessed as conservative.

In a simplified dynamic analysis, the earthquake-related design of the RPV-support structure was examined. The average loads forming the basis for the earthquake-related design of the RPV-support structure could overall be confirmed. A comparison with other load cases has shown that earthquake loads have no determining relevance for the design of the support structure. The arising higher loads are covered by the design. The investigations have yielded the result that at an earthquake intensity of I = 8 the stability can be regarded as very safe. The frequency of a loss of the load-bearing capacity of the RPV support structure due to an earthquake is estimated at $< 2 \cdot 10^{-7}$/a.

The assessment of the earthquake-related design of the piping systems inside and outside the reactor building can be summarised in the statement that in the case of an earthquake, no safety-related leakages of the feedwater-steam-circuit pipes are to be expected before there has been any relevant damage to the buildings.

Consequently, the frequencies of earthquake-induced cases where limit values are exceeded are lower for the pressure-confining piping systems than for the corresponding building regions which house any piping (i.e. $6 \cdot 10^{-7}$/a in the reactor

building and $6.3 \cdot 10^{-5}$/a in the turbine building). It is the prerequisite for the control of leaks in main-steam lines following the failure of the roof construction of the turbine building that all main-steam lines and the auxiliary steam lines are isolated by the penetration valves. An examination of the functional safety of the penetration valves of the main-steam lines (ISO-valves) showed that these are not affected even by an earthquake intensity of I = 8. As a result there is a conditional probability of $1.4 \cdot 10^{-3}$/demand for the failure of the isolating measures in at least one of five main-steam lines. Thus the contribution to the frequency of hazard states, combined with a loss of coolant outside the containment, is $< 10^{-7}$/a. After the onset of hazard states, core cooling and residual-heat removal can be maintained by shutting down the plant via the modified shutdown line. The retention of activity would, however, not be assured by this measure.

8 Summary and Conclusions

After completing the German Risk Study (Risk Study Phase B for PWR), the Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) has conducted for the first time a probabilistic safety analysis for boiling water reactors (BWR) on behalf of the Federal Minister for Research and Technology (BMFT).

The essential objective of this safety analysis is to examine the balance of safety technology, to initiate and assess safety-related improvements as well as to discuss the potential of accident-management measures.

This analysis examined selected, safety-relevant events which can lead to core damage. The examinations concentrated on plant technology. Analyses of this kind assess the frequency of events (e. g. leaks, failure of components) and the probability of failure of the safety systems then needed to control the event. A failure of such safety systems first leads to a challenge to core cooling (hazard state). After such a hazard state has occurred, accident-management measures can still be carried out in order to prevent a damage state (e. g. core damage). This analysis assesses the safety up to the hazard-state level.

The examinations take those system-related improvements and modifications of the plant operating manual into consideration which have already been implemented or will be carried out in the near future by the plant operator. The intended additional residual-heat-removal and injection system (ARHR-system) and the modified shutdown line have been assessed separately.

The potential of accident-management measures for the control of plant hazard states has been determined. By using examinations of different plants as a reference, an initial estimation of the success probabilities has been made. A quantitative assessment, however, was not made. Frequencies for damage states (e. g. core melt) were not calculated.

For accidents outside power operation, initial investigations were carried out in order to create a basis for profound analyses.

8.1 Summary of the Results

The quantitative results of the examinations are compiled in several tables and figures. In particular, they contain initiating events and their expected frequencies and plant hazard states as well as the conditional probabilities of losses of system functions. The numerical values are point values which were determined using the mean values of initiating events and the mean values of the reliability data of the components. Since the balance of the safety-related design is at the centre of the assessment, the use of point values is reasonable as the relation of the figures determined is of prime interest. A comparison with point values resulting from other studies requires some caution as no uncertainty analysis was carried out. Therefore, no statement can be made on the position of the point values in relation to the commonly used distribution measure like median and mean.

A large-scale uncertainty analysis did not seem to be justified since up to now only selected events have been examined and some phenomena which could influence the result and its uncertainty have not yet been definitely examined. Therefore, a more extensive uncertainty analysis is scheduled for Phase II of the investigations in which the derivation of bounds for the relevant phenomenological uncertainties is intended.

- **Initiating events**

Incidents and damages to components and parts of the plant that actuate the safety systems are called "initiating events". The examined initiating events and their expected frequencies are shown in Table 3-1 which groups the plant-internal initiating events as follows: operational transients, transients due to leaks in the RHR-system, anticipated transients without scram (ATWS), leaks inside the containment and leaks outside the containment.

Fire and plant-internal flooding form the group "plant-internal common-cause initiators (CCI)". Earthquakes and others (airplane crash, flooding, explosion blast wave, impacts from the neighbouring unit) are "plant-external events".

For the determination of the expected frequencies of initiating events, the following information has been used:

- plant-specific information for events for which sufficient data is available from the plant's operating experience (e.g. operational transients);
  for the loss of preferred power - which has not occurred in the reference plant - zero-event statistics are employed

- plant-specific and additional information from other nuclear power plants for events where plant-specific operating experience alone is insufficient (e.g. small leaks up to 10 cm^2)

- the methodology of the German Risk Study Phase B (DRS-B) for small (from 10 cm^2), medium-size and large leaks in pipes

- plant-specific and additional information from other nuclear power plants for events where plant-specific operating experience alone is insufficient, and model scenarios (e.g. ATWS, flooding, fire).

■ **Plant hazard states**

• Plant-internal events

To control an initiating event, certain functions of the operational and safety systems are required. These also include operator actions in accordance with the operating manual. If the basic requirements to the system functions are not met, plant hazard states occur. If, as a consequence, no accident-management measures are carried out, the plant hazard states result in damage states, e. g. core melt.

The plant hazard states are distinguished by characteristic states of the plant and by the time-span to their occurence. The plant states were classified as follows:

- b_1 Resulting from the failure of residual-heat removal, the temperature in the pressure-suppression pool exceeds 150 °C.
  Above this temperature it is not possible to operate the residual-heat-removal system. Below this temperature RPV feeding is not endangered. By heat-up and partial dryout of the pressure-suppression pool, pressure and temperature increase in the containment whose integrity will be challenged after approx. 10 h.

- b_2 In the case of failure of the steam-line isolation and RPV-feeding not being cut off, the RPV water level exceeds the level of the main-steam lines. This entails a failure of the steam line or of the adjacent systems.
  The loss of coolant after an assumed failure of the steam line leads to a rapid drop of the water level of the pressure-suppression pool and after 2 hours at the earliest to a hazard to core cooling.

- b_2^* The RPV water level of the pressure-suppression pool falls below the normal level by more than 6.5 m due to a leak in a main-steam line outside the containment and failure of steam-line isolation and subsequent evaporation of the coolant.
  In this plant state core cooling would be challenged after 2 days at the earliest.

- b_3 The RPV water level reaches the bottom of the core due to failure of RPV-feeding.

- b_4 The RPV-pressure exceeds the design pressure by a factor of 1.3 (approx. 12 MPa) as a result of the failure of the pressure limitation of the reactor-cooling circuit.

To further characterise the state of the plant, the analysis differentiates between low pressure (LP), i.e. after depressurisation, and high pressure (HP) in the RPV at the time of onset of the hazard. The hazard states have been selected in such a way that it is insignificant for their evaluation by which initiating event the state is caused.

For the examined plant-internal initiating events, Table 5-3 shows the expected frequencies of hazard states, not accounting for the ARHR-system. Table 5-4 shows the expected frequencies of hazard states with account for the ARHR-system as well as for the modified shutdown line.

Figures 5-1 to 5-3 contain further evaluations of Table 5-3. For the plant-internal initiating events, they show the contributions of individual sequence groups to the total of the expected frequencies of hazard states as well as the percentages of the various hazard states.

The frequencies of a hazard state at plant state b_2 or b_2^* for transients and for loss-of-coolant accidents inside the containment are not included in these results, since the behaviour of main-steam lines and the connecting systems after RPV excess feeding and subsequent failure of steam-line isolation (and influx of water into these lines) was not assessed. For a corroborated quantification of the conditional probability of failure of the steam lines and the connecting systems, profound plant-specific examinations are still necessary.

Nor accounting for the ARHR-system, the established point value for the total of the expected frequencies of hazard states from plant-internal initiating events is $5{,}0 \cdot 10^{-5}$/a. The result is determined about equally by the unavailability of the system functions residual-heat removal (b_1) and RPV-feeding (b_3). Approx. 90 % of the result can be assigned to event sequences which lead to a hazard after 5 h at the earliest.

Due to the diverse bypass valves, the contribution to the frequencies of hazard state b_4 (possibility of an overpressure failure) is insignificant (1 %).

Transients with failure of the main heat sink (inlcuding the case of loss of preferred power and the failure to close of a S&R valve) provide the most important contributions with about 85 %. The frequency of a hazard state for events with loss of coolant inside or outside the containment amounts to approx. $1 \cdot 10^{-6}$/a. Consequently, they do not contribute significantly to the total frequency of hazard states. In the analysis of the loss-of-coolant accidents it is assumed that the function of the RHR-system is not inhibited by loose insulation material as a consequence of the initiating event. Possibilities of clogging of strainers were already examined in the design of the plant and assessed as not being important. However, more recent operating experience questions the validity of the design assumptions. Possible effects on the function of the RHR-systems could not be examined in the framework of this analysis.

For operational transients with a failure of reactor scram (ATWS), the failure of actuation of reactor scram due to a failure of RPV water-level-measurement device is the relevant case. It leads to a hazard state of category b_3 with a frequency of $1 \cdot 10^{-6}$/a. This is especially true in the case of a failure of the main feedwater supply where the signal for reactor scram is derived only from the measurement of the RPV water level. In the long run, this case can only be controlled by manually actuating

reactor scram and RPV-feeding before the onset of core damage (approx. 10 to 15 minutes after the onset of the accident). Such manual actions have not been considered in the framework of this analysis. Hazard states can potentially occur at operational transients with mechanical failure of two or more control rods. Concerning this point, more detailed examinations are still necessary.

Additional contributions to the frequency of hazard states would arise if due to RPV excess-feeding and loss of steam-line isolation a subsequent failure of a main-steam line (state of plant b_2 or b_2^*) were to take place. The importance of these contributions depends on the conditional probabilities of failure of the main-steam lines. By means of the modified shutdown line, which was planned in connection with the ARHR-system and has already been realised, core cooling and residual-heat removal can nevertheless be maintained.

Taking account for the ARHR-system, the total of frequencies of hazard states is reduced to $4{,}4 \cdot 10^{-6}$/a (see Table 5-4 and Figures 5-4 to 5-6). Thus the total of frequencies of hazard states is reduced by a factor of 11. The ARHS-system leads to a significant improvement of the system functions residual-heat removal (b_1) and RPV-feeding (b_3). The frequency of the corresponding hazard states is thus reduced by a factor of 40 (b_1) and a factor of 7 (b_3) respectively. For all transients with loss of main feedwater supply and CCF of the RPV water-level-measurement device, the frequencies of hazard state b_3 are not reduced by the ARHR-system, since the failure of measurement also leads to a failure of signals for RPV-feeding by means of the ARHR-system. In case of a loss of preferred power with simultaneous loss of DC power supply, the ARHR-system cannot be effective, since no depressurisation can take place. The frequencies of the unassessed hazard states in category b_2 are not influenced by the ARHR-system.

Not accounting for the ARHR-system and the additional shutdown line, CCFs contribute with approx. 99 % (in the sense of importance) to the total frequency of hazard states. Failure combinations which include solely CCFs contribute approx. 80%. About 60% of the total frequency is caused by the failure to start of all three nuclear cooling-water pumps as well as of all three nuclear service-water pumps which are used directly for residual-heat removal as well as for cooling the components of the RHR-system. Approx. 20% of the result can be assigned to the

CCF with additional independent failures or/and additional failure of planned manual actions.

Due to the diverse ARHR-system, the proportion of hazard states caused exclusively by CCFs is reduced to approx. 40%. In this case, the CCF of the RPV water-level-measurement device at the loss of the main feedwater supply (ATWS) and the CCF of the 24-V-DC supply at a loss of preferred power are of importance. On the other hand, the CCFs of pumps that dominate without the ARHR-system do lead to hazard states of categories b_1 or b_3 only in combination with additional independent failures of components of the ARHR-system.

It has to be taken into account that on assessing the contribution of CCFs, generic data has been used, since methods for the determination of plant-specific data were not available. However, when checking the transferability, the plant-internal conditions were taken into consideration.

Not accounting for the ARHR-system, the proportion of erronous human actions in the unavailabilities of the system functions is relatively low (approx. 11 %); here, pessimistically assumed probabilities for errors were used for the analysis of manual actions. This small fraction is essentially due to the high level of plant automation.

- Common-Cause Initiators

The frequency of hazard states caused by flooding has been estimated at $< 10^{-7}$/a. Their contribution is thus insignificant.

Oil and cable fires in the control-rod-drive chamber of the containment have been shown to be important, but large uncertainties are associated with the quantification of the frequencies for fires inside the containment and of the conditional probabilities for the onset of a hazard state. The frequencies for hazard states due to fire inside the containment have been estimated to be well below 10^{-6}/a.

The stability and integrity of the essential buildings and components important to the safety of the plant are assured even in the extremely rare case of an earthquake of the intensity 8. The turbine building is designed deterministically to withstand intensity 7. The corresponding design limits for seismic loading are exceeded with a frequency of $6.3 \cdot 10^{-5}$/a. The frequency value determined on this basis is taken as an upper

bound for the probability of leaks in the steam lines due to a collapse of the roof construction. Non-linear plastic analyses would be required for a more precise determination of the failure probability. If steam-line isolation in at least one of the five main-steam lines fails to function correctly (conditional failure probability $1{,}4 \cdot 10^{-3}$), a loss of coolant outside the containment will occur (hazard state of category b_2^*). The corresponding frequency amounts to $< 10^{-7}$/a. Core cooling and residual-heat removal could then be ensured by a shutdown of the plant by means of the modified shutdown line. The retention of activitiy would, however, not be guaranteed.

For plant-external events like airplane crash, flooding, explosion blast wave, and impacts from the neighbouring unit, no relevant contributions to the frequencies of hazard and damage states are to be expected.

- **Accident-management (AM) measures**

In many event sequences, hazard states can be controlled and damage states be avoided by preventive AM-measures. If the failure of such measures results in a damage state, plant-internal mitigation measures can be carried out.

The accident-management manual of the reference plant describes measures for the assurance or re-establishment of

- subcriticality
- RPV-feeding at high pressure, e. g. by re-activating the main feedwater system
- RPV-feeding at low pressure, e. g. by injection with mobile pumps
- heat removal
- retention of actitivity and maintenance of the integrity of the containment, e. g. by containment venting
- power supply.

Long grace periods and various possibilities to carry out AM-measures are available in about 90% of the total frequencies of hazard states. Thus, there are favourable conditions for their successful execution. In approx. 10% of all hazard states with

short grace periods or more complicated conditions of diagnosis, only a low probability of success can be expected for the execution of AM-measures. If the examination findings from other plants are taken for a first estimation for the probability of success, the total frequency of hazard states resulting from plant-internal events amounts to < 10^{-5}/a without accounting for the ARHR-system.

For a corroborated quantification of the AM-measures, a thorough examination of the efficiency and feasibility of the measures, accounting for plant-specific conditions, is still necessary.

8.2 Conclusions

The main emphasis of the BWR safety analysis was on technical investigations of the plant. In this context, a number of essential improvements of the systems and the operating procedures for the control of accidents were recommended. These are already implemented in the plant to a large extent, leading to an increase in plant safety. Due to the plant modifications already realised and those still to be implemented, a balanced design at a high level of safety is achieved.

Examinations on the basis of the present design for the ARHR-system show that the frequency of hazard states that are connected with the failure of RPV-feeding and/or the failure of residual-heat removal can be reduced significantly by the ARHR-system. There would be a further reduction of the frequency of hazard states if an independent and diverse measurement of the RPV water level were available for the ARHR-system and if RPV-depressurisation by means of the diverse ARHR-preferred-power supply was possible. Diverse measurement could also reduce the frequency of excess-feeding transients and of the most important ATWS case.

The BWR study also showed knowledge gaps which make further examinations or developmental work necessary. For example, causal failure of main-steam lines or of the connecting systems due to excess feeding and loss of steam-line isolation might represent a significant contribution to the hazard states. The present level of knowledge, however, is not sufficient to allow a corroborated quantification of the conditional probabilities of failure of the main-steam lines and the connecting systems. For this, profound examinations would be needed. If steam-line isolation were to be improved (e. g. by diverse isolating valves, improved measurement of the RPV level),

leaks in the main-steam lines outside the containment due to excess feeding would not contribute significantly to the frequency of hazard states. In cases of hazard states with leaks in the main-steam line outside the containment, residual-heat removal and core cooling - though not the retention of activity - can be ensured by using the modified shutdown line.

For ATWS cases with mechanical failure of control rods due to common cause, which are presently regarded as being insignificant, in-depth analyses of the efficiency of residual-heat removal and the borating systems would still be necessary.

Leaks in coolant lines were not observed in the reference plant; they did, however, occur in other German BWR plants. Taking into consideration the relatively little operating experience with German boiling water reactors, it would be essential for the determination of the frequencies of small leaks to include more detailed examinations of the possible crack-formation mechanisms under special water-chemistry conditions in BWRs, going beyond the use of purely statistical data.

Furthermore, the analyses showed the large contribution of CCFs to the unavailability of the systems. A further development of the database and of the used models is inevitable. For this, it is necessary to continuously and systematically interpret the plant-specific operating experience as well as to develop models which assess on a broader basis the plant-specific counter-measures for CCFs and the measures for an early identification of CCFs.

In the consideration of AM-measures, the evaluation of human reliability will be of great importance. There is a need for research to develop simulation models by the help of which human actions, especially as a part of AM-measures, can be evaluated realistically.

Different plant states and event sequences at shutdown state have been examined in a first scoping analysis. It can be concluded that due to the characteristics of shutdown-specific conditions the analyses can turn out to be very complex and extensive. Therefore, additional profound and systematic examinations are necessary for a comprehensive assessment of the events outside power operation.

The value of the frequency of hazard states due to fire is consequently estimated well below 10^{-6}/a. In the framework of a balanced safety concept there is accordingly no need for any further fire-protection measures.

In connection with the avoidance of H_2-burn due to severe core damage, inerting the containment is discussed as a possible measure. Such a measure would also effectively prevent fires in the containment during power operation.

In order to assess the functioning of the containment at core-melt accidents in a more detailed analysis (level-2), the coolability of the core debris, e. g. in a water pool, is of decisive importance for boiling water reactors. For this reason it is necessary to set priorities for the planning and realisation of the respective research projects.

The BWR safety analysis has shown that individual results are often plant-specific and depend on technical design details. Nevertheless, the examinations also provide useful information for the assessment of other plants. Generic questions can thus be profoundly discussed.

This BWR safety analysis presents a state-of-the-art reference document as regards plant behaviour at beyond-design-basis accidents in boiling water reactors and analysis methodology; it can be used for future probabilistic safety analyses.

In summary it can be said that the present probabilistic safety analysis is a valuable instrument for the safety evaluation of boiling water reactors. Due to its systematic approach and high level of specification it has proved to be an efficient means to increase plant safety. Thus it provides an example for close-to-reality research with great benefits that can be achieved in short time.

9 References

/1/ Deutsche Risikostudie Kernkraftwerke, Phase B,
Verlag TÜV Rheinland, Köln, 1990

/2/ A.D. Swain
Accident Sequence Evaluation Program
Human Reliability Analysis Procedure
NUREG-CR-4772, 2.87

/3/ Severe Accident Risks: An Assessment for Five US Nuclear Power Plant,
Final Summary Report, NUREG-1150, Vol. 1 and 2,
Dec. 1990

/4/ Etude Probabiliste de Sûreté des Réacteurs à Eau sous Pression du Palier 900 MWe, Rapport de Synthese, IPSN, Avril 1990

/5/ M. Hirano et al.:
Recent Results of Level-1 PSA for Nuclear Power Plants in Japan; Proceedings of the OECD/CSNI Workshop on PSA Applications and Limitations, USA, September 1990, NUREG/CR-0115 (1991)

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH

Schwertnergasse 1
50667 Köln
Telefon (02 21) 20 68-0
Telefax (02 21) 20 68 442
Telex 2 214 123 grs d

Forschungsgelände
85748 Garching b. München
Telefon (0 89) 3 20 04-0
Telefax (0 89) 3 20 04 299
Telex 5 215 110 grs md

Kurfürstendamm 200
10719 Berlin
Telefon (0 30) 88 41 89-0
Telefax (0 30) 88 23 655

ISBN 3-923875-48-7