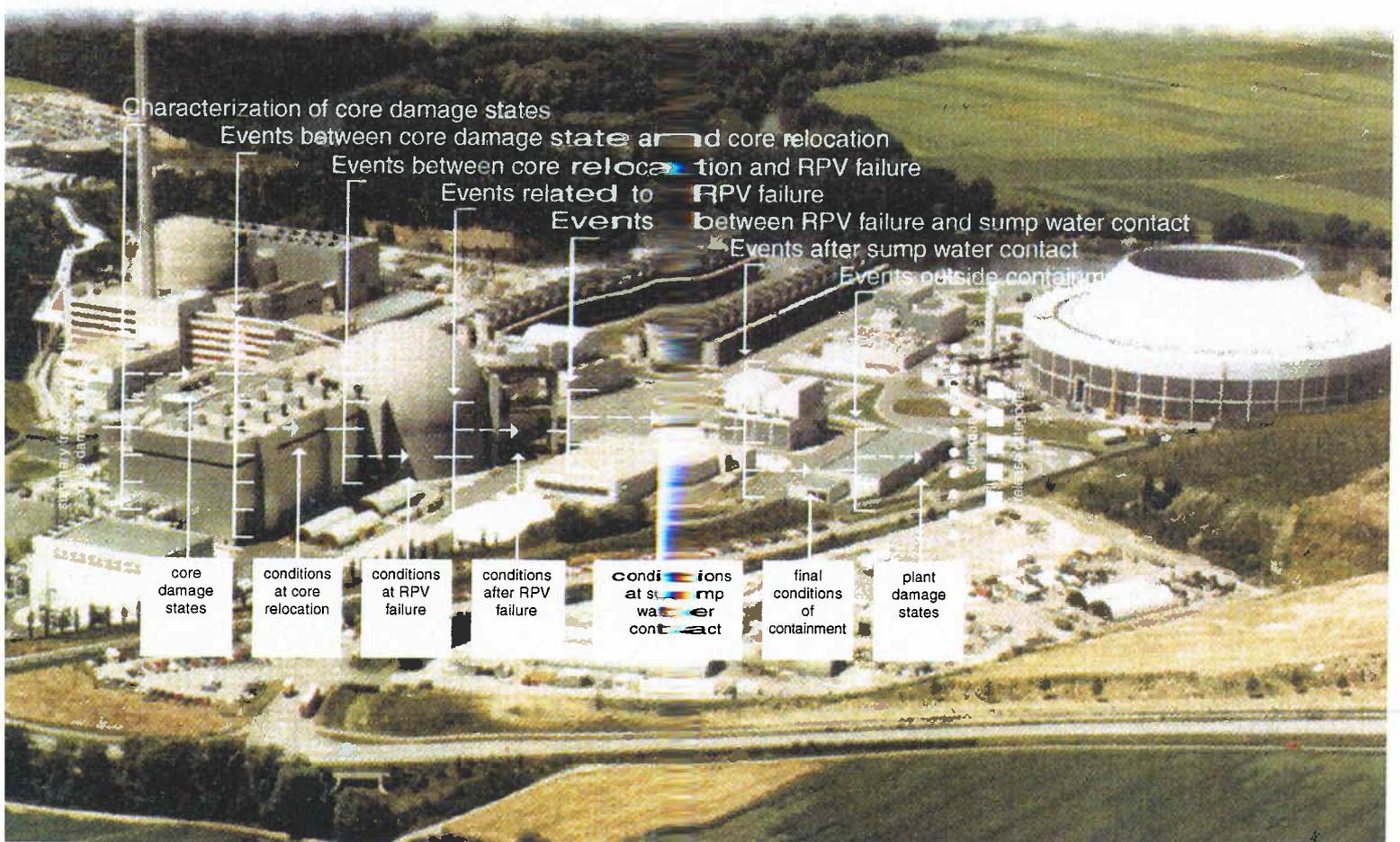


Assessment of the Accidental Risk of Advanced Pressurized Water Reactors in Germany

Methods and Results
of a Comprehensive
probabilistic Safety
Analysis (PSA)

DRAFT
FOR
COMMENT



**Assessment of the
Accidental Risk
of Advanced
Pressurized
Water Reactors
in Germany**

**Methods and Results
of a Comprehensive
Probabilistic Safety
Analysis (PSA)**

Project Leaders:

**Level 1 PSA, Power Operation:
Joachim von Linden**

**Level 2 PSA, Power Operation:
Horst Löffler**

**Level 1 PSA, LP&SD Operation:
Dieter Müller-Ecker**

**Overall Project:
Claus Versteegen**

**Report Editing:
Klaus Köberlein**

**DRAFT
FOR
COMMENT**

April 2002

**Original Report in German:
GRS-175, October 2001
ISBN 3-931995-43-7**

Remark:

This report corresponds to the technical opinion of GRS and it is not necessarily in agreement with the opinion of the client BMU.

Editorial Notes

- **Notation of numbers**

In the PSA very frequently numbers $\ll 1$ are used. It is common practice to display such numbers (as also numbers $\gg 1$) in an exponential notation. In the text of this report the common mathematical notation is used (0.00023 is displayed as $2.3 \cdot 10^{-4}$, e.g.). In tables and figures the notation common in computer printouts is used (2.3 E-4, e.g.)

- **Frequency**

The PSA calculates “expected frequencies” (also designated as “frequencies per year”), which are to be distinguished from (absolute) frequencies of certain events. Absolute frequencies can take only integer values (1, 2, 3, ...). In a given period of time, e.g., in the annual average, an expected frequency will in many cases be a non-integer value. Correctly, such frequencies are called “expected frequencies” or “frequencies per year” (or another period of time). In this report generally the term “expected” is omitted, because practically all frequencies occurring are “expected frequencies”.

- **Conditional probability**

The PSA in many instances calculates and applies “conditional probabilities”. These are probabilities which are valid in the case that a certain condition is fulfilled (e.g., the availability of a component under the condition that the normal power supply is not available). In this report generally the term “probability” is used, omitting the adjective “conditional”. The condition, under which a certain probability has been determined, usually can be inferred from the describing text.

- **Mean values representing subjective probability distributions**

The uncertainty of PSA results is quantitatively described by subjective probability distributions. It would, however, not be practicable to present all results in form of their subjective probability distribution. Therefore, in many cases the distributions are represented only by certain fractiles (5 %, 50 %, 95 %). If the result is represented by one single number, the mean value of the subjective probability distribution is used.

- **Outline of tables**

Larger tables in this report have been split into two pages in order to avoid a landscape format presentation. To improve the orientation in these tables, groups of lines are shaded (e.g. in table 5.2). The shading in these cases has no meaning with regard to the content of the table.

Descriptors:

PWR, GKN 2, core meltdown, PSA, Probabilistic Safety Assessment, accident analysis

Preface

Originally the safety of nuclear power plants was evaluated by means of purely deterministic methods. In the deterministic approach it is verified that pre-determined (“deterministic”) safety requirements are met under predefined conditions. Uncertainties of the evaluation, which are unavoidable for any kind of safety analysis, are taken into account by applying appropriate safety margins.

Since many years the probabilistic safety assessment (PSA) has been developed and applied as an important instrument for the safety evaluation, complementing – and using as a basis - the deterministic safety evaluation. The PSA is integrating the influences of system design, plant management and operational experience into a systematic approach. Furthermore the probabilistic approach is evaluating – as far as possible – the quantitative uncertainties of the analysis. The PSA is providing insights into the safety status of the plant under investigation, which cannot be gained by a purely deterministic approach. Therefore it became common practice, to use PSA for the support of safety relevant decision making.

GRS has continually developed methods for safety evaluation. The activities of GRS are related to a broad spectrum of safety relevant fields and are comprising the combination of deterministic and probabilistic methods required for a state-of-the-art safety assessment.

The operators of nuclear power plants in Germany are willing to support GRS actively in developing probabilistic methods of safety evaluation by providing the plant information required for this work. The operator of Neckarwestheim, unit 2, NPP (GKN-2) has made available to GRS not only the plant documentation but also his own PSA experience and he placed at the disposal of GRS a level 1 PSA for GKN-2, performed as part of the Periodic Safety Review, together with all related documentation.

GRS took advantage of these favorable conditions for the application and evaluation of probabilistic methods, developed in various projects, by taking GKN-2 as reference plant for a comprehensive PSA, into which the inputs from these projects have been integrated. The present report is describing the investigations and the results of this PSA, without identifying any demarcation between contributing projects. The following

projects, performed by GRS on behalf of the BMU, have contributed: SR 2259, SR 2356, SR 2274, SR 2276, SR 2303, SR 2306, SR 2307.

In this way a PSA, comprehensive as far as possible according to the current state-of-the-art, for a German NPP with pressurized water reactor has been made available. The methods which have been evaluated by performing a complete PSA for an advanced PWR can be applied by a wide circle of users with according experiences. This was facilitated by the funding from BMU to GRS and by the willingness of the operator of the reference plant GKN 2 to cooperate with GRS. We like to express our thanks for this support also in this place.

Furthermore we thank all colleagues in GRS who participated in performing the PSA and contributed to the present report.

This report, which is available in German and English, is presenting the methods and the results of the PSA to the experts and to a broader public. GRS invites interested persons and institutions in Germany and abroad to critically review and comment the PSA. We intend to evaluate critical comments and to consider them in a revised version of the PSA.

Table of Contents

1	Introduction	1
2	Objectives of the study.....	5
3	Reference plant	7
3.1	Introduction	7
3.2	Layout and function of a nuclear power plant with pressurized water reactor (PWR)	8
3.3	Safety concept	9
3.4	Safety relevant systems and components.....	11
3.5	Specific features of the Convoy plants	13
3.6	Specific features of GKN 2 compared to the Convoy standard.....	15
4	PSA approach.....	17
4.1	Introduction	17
4.2	Scope and methods of the present PSA	20
4.3	Characteristics of the “Basis-PSA”	22
4.4	Modifications of the Basis-PSA	25
4.4.1	New evaluation of the influences from common cause failures (CCF) of redundant components	25
4.4.2	Consideration of plant internal accident management	26
4.4.3	Consideration of repair of failed components.....	26
4.4.4	Evaluation of plant specific component reliability data	27
4.4.5	Modification of event tree and fault tree analyses	28
4.4.6	Evaluation of probability distributions and mean values.....	28
4.4.7	Events during low power and shutdown states	29
4.5	Extension of the PSA by fire analyses	29
4.5.1	Selection of fire risk relevant areas (Screening).....	29
4.5.2	Frequency of fires	30
4.5.3	Evaluation of fire consequences	30
4.5.4	Event tree and fault tree analyses.....	31

4.5.5	Fire effects on the technological systems	31
4.5.6	Summary of the results of the fire analysis	32
5	Level 1 PSA for power operation.....	35
5.1	Initiating Events.....	35
5.1.1	Investigated initiating events and their frequencies.....	40
5.1.2	Estimations for events not investigated in detail	47
5.2	Transition from initiating events to system damage states.....	61
5.2.1	Small leak at a main coolant line, 80 - 200 cm ²	67
5.2.2	Small leak at a main coolant line, 25 - 80 cm ²	74
5.2.3	Small leak at a main coolant line, 2 - 25 cm ²	78
5.2.4	Small leak at the pressurizer by stuck open safety valve.....	81
5.2.5	Steam generator tube leak, 1 - 6 cm ²	83
5.2.6	Loss of preferred power	87
5.2.7	Loss of main feedwater without loss of main heat sink	90
5.2.8	Loss of main heat sink without loss of main feedwater	93
5.2.9	Loss of main feedwater and loss of main heat sink.....	95
5.2.10	Main steam line break outside the containment.....	97
5.2.11	Main feedwater line break outside the containments	99
5.2.12	Synopsis of the results for system damage states	102
5.2.13	Estimations concerning initiating events not analyzed in detail.....	106
5.3	Transition from system damage states to core damage states.....	108
5.3.1	Prevention of core damage states	108
5.3.2	Characterization of the core damage states.....	110
5.3.3	Contributions of initiating events to core damage states.....	116
5.3.4	Summary of the results for core damage states.....	149
5.4	Uncertainties of the results of the reliability analysis.....	157
5.4.1	Results of the uncertainty analysis for system damage states.....	161
5.4.2	Results of the uncertainty analysis for core damage states	167
5.5	Insights with respect to the PSA methods and to the plant design	173
5.5.1	PSA methods	173
5.5.2	Plant design	174

6	Level 2 PSA for normal power operation	177
6.1	Introduction	177
6.2	Exemplary description of two accident progressions	178
6.2.1	Slow accident evolution after core melt with low pressure in the primary system	179
6.2.2	Fast accident progression after core melt at high pressure	183
6.3	Event tree analysis	188
6.3.1	Core damage states in the event tree	188
6.3.2	Set-up of the event tree	190
6.4	Ultimate containment strength during pressurization	195
6.5	Containment loads	196
6.5.1	Impact of steam explosions inside the reactor pressure vessel	197
6.5.2	Containment load due to hydrogen	200
6.5.3	Pressure rise inside the containment upon reactor pressure vessel failure	202
6.5.4	Melt spread in the lower part of the containment	205
6.5.5	Load and failure of sump suction pipes	207
6.5.6	Erosion of the concrete foundation	209
6.5.7	Filtered venting of the containment	210
6.6	Results of the event tree analysis and their relation to initiating events..	212
6.6.1	Final location of the core materials	213
6.6.2	Pressure inside the reactor coolant loop immediately before RPV failure	214
6.6.3	Final status of the containment	217
6.6.4	Release paths and release categories for radionuclides	218
6.7	Uncertainty of results	224
6.8	Findings related to PSA methods and to plant performance	227
6.8.1	PSA methods	227
6.8.2	Plant performance	228
7	Level-1 PSA for low-power and shutdown operation	233
7.1	Introduction	233

7.2	Plant operational states.....	234
7.3	Initiating events	235
7.3.1	Analyzed initiating events and their probabilities.....	241
7.3.2	Estimates on events not or not completely analyzed events.....	248
7.4	Transition from initiating events to system damage states.....	255
7.4.1	Reliability data	258
7.4.2	Loss of preferred power - external (mid-loop-operation, RPV closed)	263
7.4.3	Loss of preferred power (mid-loop operation, RPV open).....	266
7.4.4	Loss of RHR by faulty water level lowering (water level lowering to mid-loop operation, RPV closed)	268
7.4.5	Loss of residual heat removal by operational failure of the residual heat removal chains (mid-loop operation, RPV closed)	270
7.4.6	Loss of residual heat removal by failure of the RHR chains during operation (mid-loop operation, RPV open).....	272
7.4.7	Loss of residual heat removal by faulty actuation of the emergency core cooling signals (mid-loop operation, RPV closed).....	274
7.4.8	Leak at the residual heat removal system in the containment and in the annular room < 25 cm ² (mid-loop operation, RPV closed)	276
7.4.9	Leak at the residual heat removal system in the containment and in the annular room < 25 cm ² (mid-loop operation, RPV open)	278
7.5	Summarized explanations concerning the system damage states	280
7.6	Uncertainties of the reliability analysis	283
7.7	Findings related to PSA methods and systems engineering.....	285
7.7.1	PSA methods	285
7.7.2	Systems engineering.....	294
8	Summarized evaluation and conclusions.....	296
8.1	Insights related to the available PSA methods.....	296
8.1.1	Results of the evaluation of PSA methods.....	296
8.1.2	Conclusions concerning the evaluation of methods.....	302
8.2	Conclusions related to the safety of the reference plant	305
8.2.1	System and core damage states.....	305
8.2.2	Plant damage states	306

8.3	General conclusions.....	308
9	References.....	310
	List of figures	319
	List of tables	321

1 Introduction

The safety design of nuclear power plants follows a “defense-in-depth” concept in a double meaning: the radionuclides produced in the reactor core are confined by several barriers, the integrity of the barriers is protected by multistage measures.

The radionuclides are confined by following barriers: the cladding of the fuel rods, the pressure boundary of the reactor cooling system, and the containment. The measures to protect the barriers are categorized into four levels with the following tasks:

- level 1: to prevent disturbances of the normal operation
- level 2: to cope with incidents and to prevent accidents
- level 3: to cope with accidents
- level 4: to prevent severe accidents and to mitigate consequences of severe accidents.

In Germany level 4 is split into

- level 4a: measures to cope with extremely remote events (ATWS and emergency states)
- level 4b: preventive (plant internal) accident management
- level 4c: mitigative (plant internal) accident management.

ATWS stands for anticipated transients with failure to scram, i.e. transients which – due to their estimated frequency - are expected to occur during the operational lifetime of the plant, combined with a failure of the reactor scram required to cope with the transient. “Emergency states” (in German: “Notstandsfälle”) are external, man-made area events like airplane crash or chemical explosion.

The safety level of a nuclear power plant is given by the design of operational and safety systems, by the operational management and by the operational proof of activity barriers and protection measures. The PSA integrates the influences, essential for the plant safety status, from system engineering, operational management and operational experience into a systematic approach and it quantitatively evaluates the uncertainties of the analysis. The probabilistic safety evaluation refers to the following relations between the multistage safety concept and PSA results:

If – with relation to the defense-in-depth concept – the operational and safety related measures on the first three levels to ensure sufficient cooling of the reactor core are not available to the required extent or are not efficient in case of demand, the plant is in a damage state of the safety system (system damage state). In this state core meltdown can still be prevented by further protection measures. If also the protection measures of the levels 4a and 4b are either not sufficiently available or not efficient in case of demand, a core meltdown will occur as soon as the nuclear fuel reaches the melting temperature (core damage state). The radiological consequences of a core meltdown can be mitigated by the safety measures of level 4c. The purpose of these measures is to prevent a failure of the containment (plant damage state) as a consequence of the core damage.

Therefore the frequency of system damage states, as evaluated in the PSA, characterizes the quality of the first three safety levels for the prevention of a core damage, i.e. the "classical" safety design of the nuclear power plant. The frequency of core damage states additionally comprehends the protection measures to prevent core meltdown on the fourth level of safety. Finally, the frequency of plant damage states characterizes the quality of all protection measures, which prevent a core meltdown with a large release of radioactive material into the environment.

Thus, the frequencies of system, core, and plant damage states provide criteria for the actual safety status of a plant.

It is common practice to distinguish three levels of a PSA. Level 1 analyzes, and quantifies the frequency of, event sequences until core meltdown. Starting from the core damage states and the phenomena characteristic for these states, the level 2 of the PSA analyzes event sequences until plant damage states and quantifies the frequencies of these states. While a level 1 PSA essentially is based on technical experience, the level 2 has to deal predominantly with effects and phenomena beyond technical experience and therefore has to rely largely on the computer simulation of complex physical-chemical processes and on expert judgement. Finally, in level 3 of a PSA extent and expected frequency of health, environmental, and property damages are evaluated, which can be caused by the radionuclides released from the plant during an accident.

Up to now PSAs for nuclear power plants in Germany have generally been restricted to the quantification of system damage states from events occurring during normal power

operation. They have been performed by the utilities, and reviewed by technical safety organizations as part of the "Periodical Safety Review (PSR)" for all nuclear power plants in Germany according to the guidelines for the performance of the PSR published by the BMU. After completion of Phase B of the German Risk Study in 1990 GRS has further developed PSA methods and evaluated these methods in limited projects as well for low-power and shutdown states as for the quantification of core and plant damage states. However, a comprehensive PSA, analyzing the initiating events continuously over the levels 1 and 2 for normal power operation and for low-power and shutdown states, was not yet performed. Therefore in Germany, different from other countries, a sufficiently approved methodology for this purpose was not available. This means that the safety evaluation approach in Germany is not in full compliance with the international state of the art. This finally was the motivation for GRS, to test and to approve the available probabilistic methods by a comprehensive and continuous level 2 PSA.

2 Objectives of the study

The objective of the study was to evaluate the available PSA methods and to demonstrate their usability for practical applications by performing a comprehensive PSA for an advanced German PWR.

Based on a PSA performed for the reference plant GKN 2 as part of the Periodical Safety Review ("Basis-PSA") the following tasks had to be performed:

- modification and completion of the event tree and fault tree analyses for the initiating events considered in the Basis-PSA,
- investigation and estimation of the risk contribution from area events,
- comprehensive consideration of preventive plant internal accident management and exemplary consideration of repair after accident initiation,
- investigation of accidents during low power and shutdown states,
- investigation of core damage events caused by accidents during normal power operation and failure of required safety functions,
- consideration of mitigating measures of the plant internal accident management,
- quantification of uncertainties of analytical results as comprehensively as possible.

3 Reference plant

3.1 Introduction

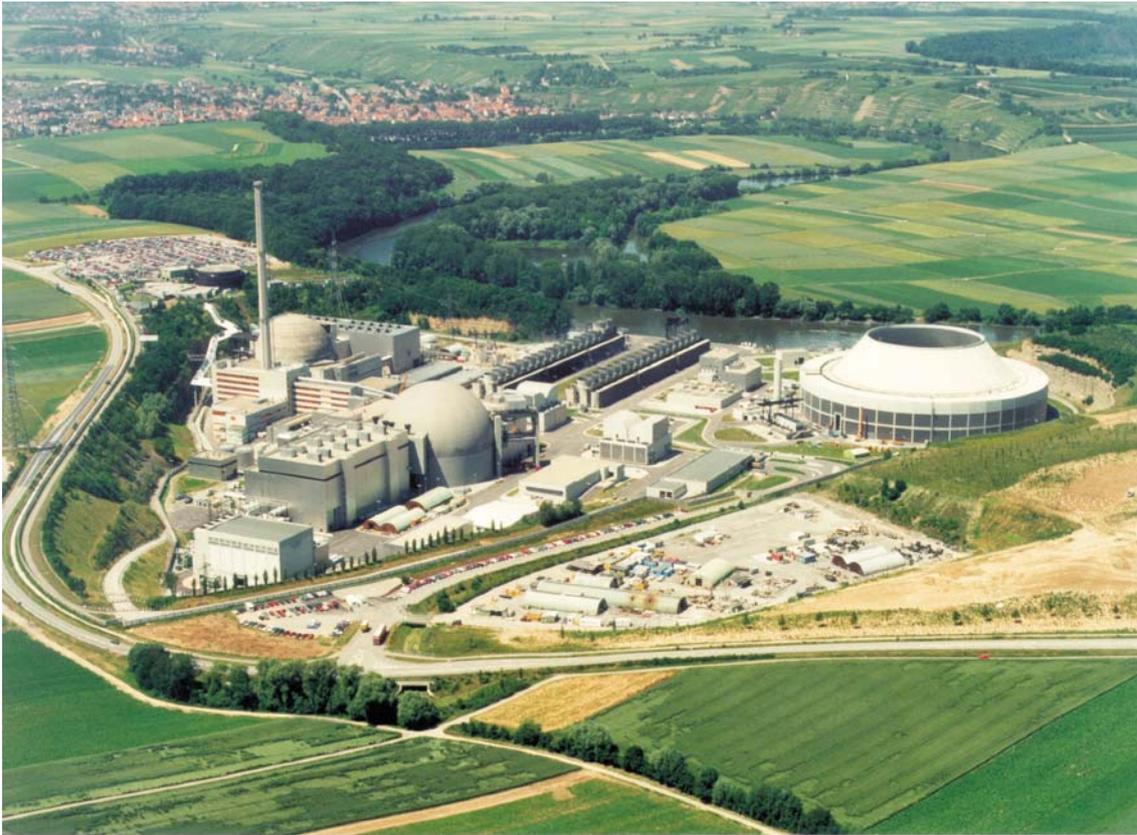
Reference plant of the present PSA is Gemeinschaftskernkraftwerk Neckar, unit 2 (GKN 2). Together with KKI 2 (Isar NPP, unit 2) and KKE (Emsland NPP) GKN 2 belongs to the group of three 1300 MWe NPPs, which have been built as “Convoy-Plants” within a short period of time and with nearly identical design. GKN 2 has been commissioned as the latest of the “Convoy-Plants” in April 1989. Shareholders of the operating company, the Gemeinschaftskernkraftwerk Neckar GmbH, are Neckarwerke Stuttgart (70 %), Deutsche Bahn (18.2 %), Energie Baden-Württemberg (9.1 %) and Zementwerk Lauffen – Elektrizitätswerk Heilbronn (2.7 %).

GKN 2 is located next to GKN 1 (PWR, 2500 MWth, 835 MWe) at the bank of river Neckar in a closed down stone-pit within the boundary of the community of Neckarwestheim. Fig. 3.1 gives an overview on both plants at the site (unit 2 in the front).

The reactor of GKN 2 has a thermal output of 3850 MW. The installed electrical gross power has been increased from originally 1316 MW to now 1365 MW. The electrical net output (gross output minus electrical house load) is 1269 MW. Since the date of commissioning (April 15, 1989) until end of 2000 GKN 2 has delivered 121 TWh electrical energy into the grid, according to a load factor of 93.6 %. In the same period of time the time and work availability was above 96 %, the highest operational reliability of all nuclear power plants in Germany.

The utility has made available to GRS all documentation and information required for the PSA and, additionally, the PSA which had been performed by Siemens-KWU on behalf of the utility for the Periodic Safety Review.

The following chapters describe in short the layout and function (chapter 3.2), the safety concept (3.3), and safety relevant systems and components (3.4) of a NPP with PWR and the technical and organizational status of the reference plant as analyzed in the PSA.



(Source: GKN)

Fig. 3.1 Overview on GKN NPP units 1 and 2

3.2 Layout and function of a nuclear power plant with pressurized water reactor (PWR)

Figure 3.2 shows the functional schema of a PWR.

The heat produced in the fuel elements by nuclear fission and radioactive decay is transferred by the reactor cooling circuit (primary circuit) from the reactor pressure vessel via steam generators to the feedwater-steam circuit (secondary circuit). The water used as reactor coolant is under high pressure (about 15.8 MPa), so that it does not evaporate even at a maximum temperature of about 326 degree C (at the outlet of the reactor core). The term “pressurized water reactor” has been coined to describe this circumstance. Main coolant pumps forward the reactor coolant along the primary circuit. The water, which is fed into the secondary side of the steam generators by feedwater pumps, is evaporated by the heat transferred from the reactor cooling circuit. The steam produced in the steam generator propels the turbine and the generator. In this way part of the thermal energy of the steam is transformed via mechanical (rotation)

energy into electrical energy. The remaining steam, whose thermal energy cannot be transformed into mechanical energy, leaves the turbine and is condensed to water in the condenser. The waste heat from the condensed steam is transferred via the cooling water circuit (tertiary circuit) and the cooling tower into the environment.

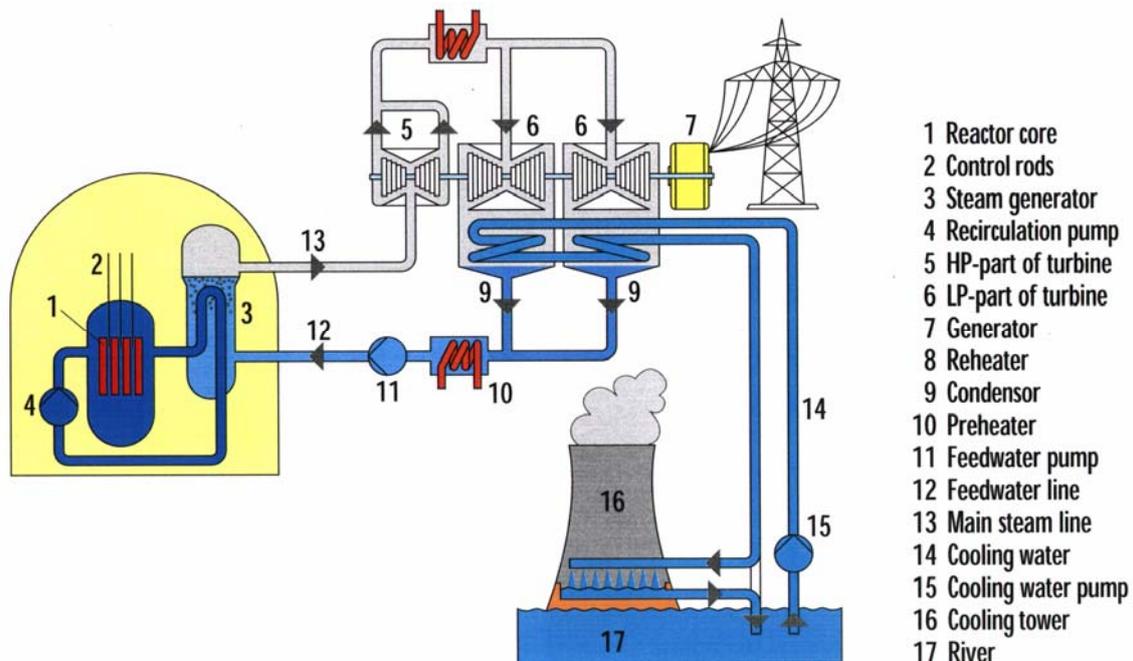


Fig. 3.2 Functional scheme GKN 2

3.3 Safety concept

During reactor operation the nuclear fission generates a great amount of radioactive fission products within the reactor core as undesired, yet unavoidable by-product. To a far less amount radionuclides are produced by the activation of nuclear fuel and structure material. In order to avoid a release of radioactive substances, which are dangerous for man and environment, two basic principles are applied: the radionuclides are confined by several structures - the "activity barriers" - and the barriers are protected by multistage measures (defense-in-depth).

In a PWR the radionuclides are confined by the following barriers: the gas-tight cladding of the fuel rods, by the closed structure of the reactor cooling circuit, and by the containment, enclosing the whole reactor cooling circuit.

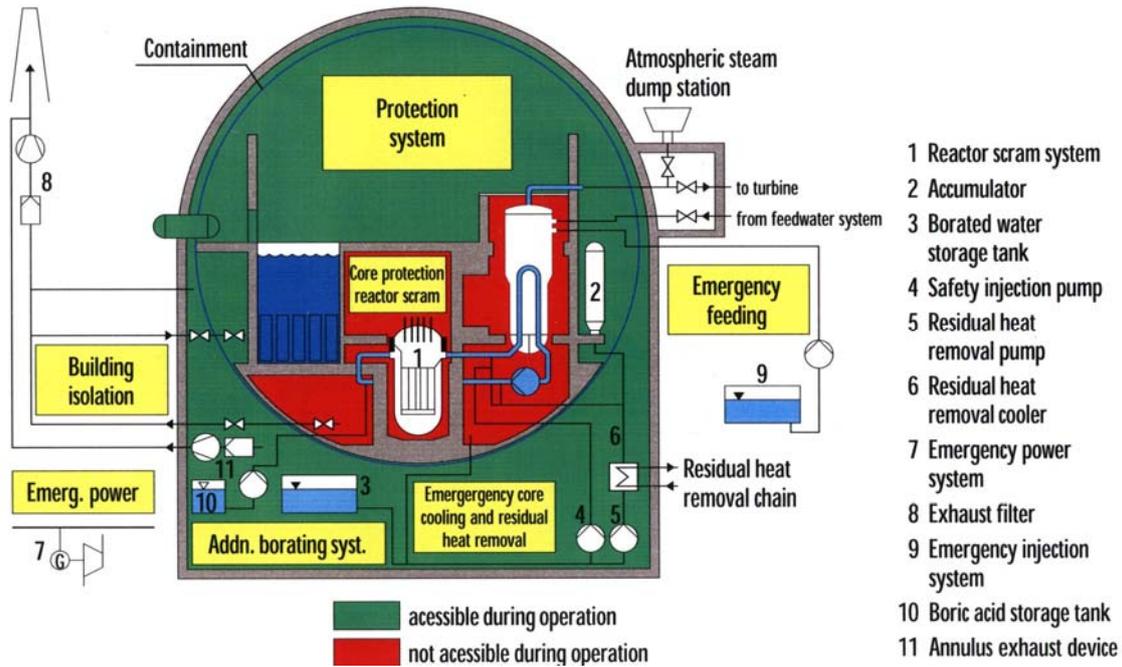


Fig. 3.3 Scheme of the principal safety installations of a PWR

The first level of measures to protect the activity barriers is realized by high quality standards of all components and systems of the plant. In this way operational disturbances, which could escalate into accidents, are avoided as far as possible. Operational disturbances, which occur in spite of these provisions, are controlled – on the second level of the defense-in-depth concept – by protection and limitation devices, before they can escalate into accident. The third level is realized by safety systems, which cope with accidents by scrambling the reactor and by removing the decay heat which unavoidably is produced even after the nuclear fission has been stopped and the reactor is shut down. A spectrum of “design basis accidents” is defining the requirements concerning the safety systems. On a fourth level, finally, additional measures are realized against events, which are not design basis accidents due to their very low expected frequency of occurrence. Furthermore, on this level plant internal accident management measures are provided, in order to make possible the cooling of the reactor core by a flexible use of available system functions even after a failure of safety systems or – as “ultima ratio” measures – to mitigate the consequences of a core damage.

The safety systems, provided to cope with design basis accidents, are to be realized with high reliability. Therefore, these systems are designed to be redundant, i.e., there are more system trains available than are required to perform the intended system

function. The redundant system trains – as far as possible – are functionally independent and physically separated from each other, and – if necessary – protected by building structures. Most of the essential safety functions are actuated and controlled automatically. Actions of the operating personnel are not required within the first 30 minutes after the initiation of an accident.

3.4 Safety relevant systems and components

In the following, short descriptions of the safety relevant systems and components of a PWR are given:

- In the reactor core, situated within the reactor pressure vessel, the energy released by the nuclear fission is transformed into heat. Most of the radioactive material present in the plant is concentrated in the reactor core.
- The reactor cooling circuit is composed of the reactor pressure vessel, the hot and cold legs of coolant loops, the primary side of the steam generators with the steam generator tubes and the inlet and outlet chamber, the main coolant pumps and the pressurizer. The heat transferred to the water in the reactor core is transported to the steam generators via the reactor cooling circuit. In the top area of the pressurizer there is a steam volume, in order to allow contraction and expansion of the reactor coolant without significant variations of system pressure.
- By neutron absorbing control rods, which can be inserted into the reactor core from the top, the heat generation and the power distribution in the reactor core can be controlled and the reactor can be shut down by interrupting the nuclear chain reaction. By adding a neutron absorber (boron) to the reactor coolant a long term control of fission power produced in the core is realized. The decrease of reactivity caused by the burn-up of the nuclear fuel can be compensated by a reduction of the boron concentration.
- The reactor scram system (see fig. 3.3, No. 1) allows a fast interruption of the nuclear chain reaction by the insertion of control rods. In this way the energy production in the reactor is reduced to the decay heat level within a few seconds. Ten seconds after a reactor scram the decay heat is about 10 % of full power. It decreases continuously, but relatively slowly (after 1 hour: about 1 %, after 1 day: about 0.3 %).

3 Reference plant

- The feedwater-steam circuit is composed of the secondary side of the steam generators, the steam lines with the steam bypass system, the turbine with the turbine condenser and the main condensate pumps. During power operation the steam is transported in the steam lines from the steam generators into the turbine. The steam leaving the turbine is condensed in the turbine condenser. The condensate is transported into the feed water tank and from there via the feedwater lines into the steam generators.
- The volume control system with the chemical control system compensates volume contractions and expansions of the reactor coolant inventory, and it allows to adjust the boron concentration in the reactor coolant to a given value
- The reactor protection system supervises all safety relevant process variables and
 - at the onset of limit values - it activates reactor protection signals, which trigger safety actions like reactor scram, emergency core cooling and emergency steam generator feeding (see fig. 3.3).
- The limitation devices and control systems – including the reactor protection system – have the purpose to keep process variables, important for the reactor operation and the safe state of the plant, within prescribed boundaries
- The electrical power supply is composed of the preferred power supply (for house load) and emergency power supply (see fig. 3.3). The preferred power supply, which can be fed from the main generator and from the external grid, is serving operational and safety relevant consumers. After a loss of preferred power supply electrical power to safety important components is provided by diesel driven generators. Safety important components, which need to be supplied without interruption (mainly instrumentation and control systems) are served by accumulators during start-up of the diesel generators.
- The emergency core cooling and decay heat removal system comprises the functions high pressure injection (fig. 3.3, No. 4), accumulator injection (fig. 3.3, No. 2), low pressure injection (fig. 3.3, No. 5). During normal shutdown phases its task is the long term decay heat removal via heat exchangers (fig. 3.3, No. 6), the component cooling system, and the service water system. In case of a loss-of-coolant accident it can feed water into the reactor coolant circuit, first taking suction from borated water storage tanks (fig. 3.3, No. 3) and from the accumulators (Fig. 3.3, No. 2), after the storage tanks are empty from the containment sump.

- The emergency feedwater system (fig. 3.3, No. 9) feeds the steam generators after a failure of the main feedwater system. The emergency feedwater system can be applied for decay heat removal and to cool down the plant.
- The emergency system (in German: Notstandssystem) has the task to maintain vital safety functions (subcriticality, decay heat removal) for at least ten hours after a failure of systems which are not physically protected against external impacts.
- The pressure resistant and technically gas-tight containment (design pressure 0.63 MPa absolute, design leakage < 0.25 vol. % / day) encloses the most important systems containing radioactive material. The containment function is supported by the valves of the containment isolation system. The containment is designed to withstand pressures and temperatures to be expected during a loss-of-coolant accident. In the containment sump the water draining from the primary circuit in the case of a loss-of-coolant is collected. The surrounding reinforced concrete shell (wall thickness up to 1.8 m) protects the containment against external impacts. The annular room between containment and reinforced concrete shell can be kept under sub atmospheric pressure by a ventilation system. The air – ventilated from the annular room – is blown into the atmosphere via filters and the stack (fig. 3.3, No. 8).

3.5 Specific features of the Convoy plants

The Convoy plants are the latest generation of pressurized water reactors in Germany. Their concept and construction used experiences from the construction and operation of preceding plants and – concerning the safety design – took into account insights from the German Risk Study in a consistent manner.

Applying the Convoy concept the construction time which had increased to about 80 months for the preceding plants (Brokdorf/KBR, Philippsburg 2/KKP 2, Grafenrheinfeld /KWG) was reduced to about 60 months. This was realized mainly by the following measures /KEL 88/:

- Rationalization and optimization of the licensing procedure
More stringent, but for all projected plants unified requirements have been preferred to possibly reduced but site specific requirements (i.e., with regard to seismic design). The licensing procedure has been split into three steps for the con-

3 Reference plant

struction permit and the operation license compared to 15 steps with the preceding plants.

- Detailed and comprehensive pre-planning

For the Convoy plants the pre-planning was completed to 95 % at the beginning of the construction, while for Philippsburg NPP, unit 2 (KKP 2), this status was reached about 3.5 years after beginning the construction. The planning has been efficiently supported by a mock-up, scaled down 1:25, for the most important buildings.

In this way the expenditures for modifications during the construction phase were reduced considerably (for KKI 2 to about 4 % of the expenditures for KKP 2).

- Detailed planning and optimized realization of construction and assembling

By using enlarged pre-fabricated units the total number of on-site welding seams at pipes was reduced significantly.

The approaches described above, did help not only to reduce the construction time and costs, but also to improve the quality and the safety of the plants.

Most of the safety relevant design improvements have been realized also for older plants. For the pre-Convoy plants they have been realized during construction, for the Convoy PWRs most of the improvements have been taken into account during the planning phase. They comprise the following points:

- Basically safe design of the pressure boundary of the reactor coolant circuit (“leak before break”),
- functional separation of operational systems from safety systems,
- local and functional separation of redundant strands of safety systems,
- increased degree of automatization,
- increased redundancy of steam generator feedwater supply and steam relief,
- improved energy supply by main and reserve grid connections and two independent emergency power systems,
- improved specification of components (including instrumentation) to cope with accidental environments,
- securing of manually operated valves,

3.6 Specific features of GKN 2 compared to the Convoy standard

- improved man-machine communication (PRISCA = Process Information System, Computer Aided),
- protection goal oriented operator manual, supplementing the event oriented operator manual,
- system design and organizational modifications related to plant internal accident management (upgrading of components, emergency manual). These improvements have been planned during commissioning phase and realized during the first refueling outage.

When the Convoy plants were commissioned (1987 – 1989) they defined the state of the art in reactor safety in Germany, which also gave the basis for the German nuclear rules and regulation (“KTA-Regeln”).

The progression in the state of knowledge in nuclear safety technology did require backfitting of Convoy plants only in a few points. Examples are the improvements of the interface between high pressure and low pressure sections of the primary coolant circuit, realized after the event of December 17, 1987 in Biblis, unit A, NPP /HÖR 89/, and improvements with respect to plant internal accident management (primary side bleed, hydrogen recombination, equipment for the filtered venting of the containment atmosphere).

3.6 Specific features of GKN 2 compared to the Convoy standard

Although the three Convoy plants are uniform as far as possible, site specific conditions and specific requirements of the respective utilities in some points caused deviations from the standard /GRS 90/. GKN 2 has specific features mainly in the following points:

- The waste heat is dumped into the environment in a closed main coolant circuit via a hybrid cooling tower without thermal pollution of the river Neckar. The cooling tower can be operated as wet cooling tower or as wet-dry cooling tower (“hybrid cooling tower”). Advantages of a hybrid cooling tower are its significantly lower height and its much lower production of vapor compared to a wet cooling tower. The operational statistics of GKN 2 show that the cooling tower is used nearly exclusively in hybrid mode. The other Convoy plants, like most other German NPPs, are equipped with wet cooling towers.

3 Reference plant

- On the site of GKN is a building with a transformer station to generate electric power for the German railway grid (16 2/3 Hz, 110 kV, 2 x 75 MW rated power).
- The main coolant pumps of GKN 2 have been produced by Andritz, while KSB pumps are installed in KKI 2 and KKE.
- The design of the first reactor core has been modified compared to the cores of KKI 2 and KKE, in order to minimize neutron leakage (“low-leakage core”).
- The I&C system has been modified in order to allow stretch-out operation with reduced coolant temperature.

Furthermore, due to the erratic topography at the site of GKN 2 with varying heights and refilling areas as a result of the preceding stone-pit operation very high foundation efforts were necessary, which extended the overall construction time by about one year. The foundation material was required to have the same properties regarding seismic effects as the surrounding natural ground.

The specific features of GKN 2, mentioned in this chapter, did not influence the approach and the results of this PSA.

4 PSA approach

4.1 Introduction

The methods of a PSA are described in numerous publications (e.g., /GRS 90/); therefore they are outlined here only in short.

It is common practice to distinguish three levels of a PSA.

A level 1 PSA evaluates the frequency of a core meltdown. The accidental risk of a nuclear power plant is determined by such events which lead to a meltdown of the reactor core – and hence to a failure of the inner activity barrier (fuel rod claddings). Therefore a level 1 PSA starts with the identification of initiating events, which after a failure of safety systems can lead to a meltdown of the reactor core. Then, by means of event tree and fault tree analyses, the expected frequency of a core meltdown is calculated.

A PSA which – according to the requirements of the German PSA Guideline – investigates also the availability of the active functions of the containment is designated as Level 1+ PSA.

Different from the international practice it is common in Germany to display also the frequency of system damage states as result of a PSA. System damage states occur if system functions for the cooling of the core, which according to the safety design are required to cope with accidents, are not available. In this case a core meltdown can be prevented only by plant internal accident management or by repair of failed components. The frequency of system damage states is a measure for the safety level of the plant realized within the design basis – not taking into account plant internal accident management.

A level 2 PSA – based on the results of the level 1 – investigates the probability of a containment failure after a core meltdown and the extent of radionuclide release into the environment after containment failure

In a level 3 PSA – based on the results of the level 2 – extent and probability of external damages are evaluated.

4 PSA approach

Up to now in Germany mainly level 1+ PSAs without consideration of plant internal accident management have been performed. The PSAs performed as part of the Periodical Safety Review for all German nuclear power plants did investigate a broad spectrum of plant internal initiating events, including flooding. Other internal and external area events have not been investigated or only by means of rough estimates. The analyses started from the assumption, that at onset of an accident the plant is in power operation. Accidents during non-power operation, i.e. during shutdown, start-up or an outage, have been investigated by research projects for selected events in a PWR and a BWR.

For all plants investigated the estimated overall frequencies of states with a violation of the design basis for the core cooling (system damage states, formerly also designated as system damage states) have been – in most cases significantly – lower than $10^{-4}/a$. In cases where the effect of plant internal accident management has been taken into account the overall core damage frequencies were below $10^{-5}/a$.

A level 2 PSA was intended to be performed by Phase B of the German Risk Study. The response of the containment after a core meltdown has been investigated by means of the methods available at that time (until 1989). However, probabilities for the various failure types of the containment have not been quantified, because the computer codes simulating the phenomena after a core meltdown were considered not to be sufficiently reliable.

The approach of a level 2 PSA is different from the approach of a level 1 PSA in important points. The level 1 analyses are characterized by the following situation:

- The plant configuration is close to the “normal” state.
- Event sequences are determined by the functioning resp. failure of design basis system functions (and the availability of preventive plant internal accident management measures).
- The failure probabilities of the system functions required to cope with an initiating event – and hence the probabilities for the branchings in the event trees – can in most cases be determined by means of fault tree analyses.
- The analysis – at least in part – is supported by operational experience (failure probabilities of components, frequencies and time histories of accidents).

Thus the level 1 of the PSA is “system oriented”, and its quality to a considerable degree depends on the availability of data on the reliability of safety relevant components.

The level 2 of the PSA requires a different approach in a number of points:

- The plant status will more and more depart from the status as designed – also with respect to plant geometry. This is especially true after a failure of the reactor pressure vessel.
- The accident sequences in most cases do not depend on the function of certain systems – with the exception of mitigating plant internal accident management measures -, but mainly from the development – or the occurrence or non-occurrence – of physical-chemical processes (e.g., steam explosion, extent of generation and mode of distribution of hydrogen, sources of ignition).
- The analyses have to be based nearly exclusively on the computer simulation of accident sequences.

Thus the level 2 of the PSA is mainly characterized by accident phenomena, and its quality depends first of all on the simulation of processes inside the containment after a core melt accident.

Phase B of the German Risk Study has been published more than 12 years ago. In the meantime – supported by experiments - considerable improvements have been realized concerning the simulation of core meltdown accidents and related phenomena inside the containment. The methods have been evaluated for selected problems as part of the BWR Safety Study /GRS 93/. By the present level 2 PSA for a large PWR the current state-of-the-art in various fields has been brought together in an analysis which is comprehensive as far as possible.

4.2 Scope and methods of the present PSA

Fig. 4.1 shows the scope of the present level 2 PSA.

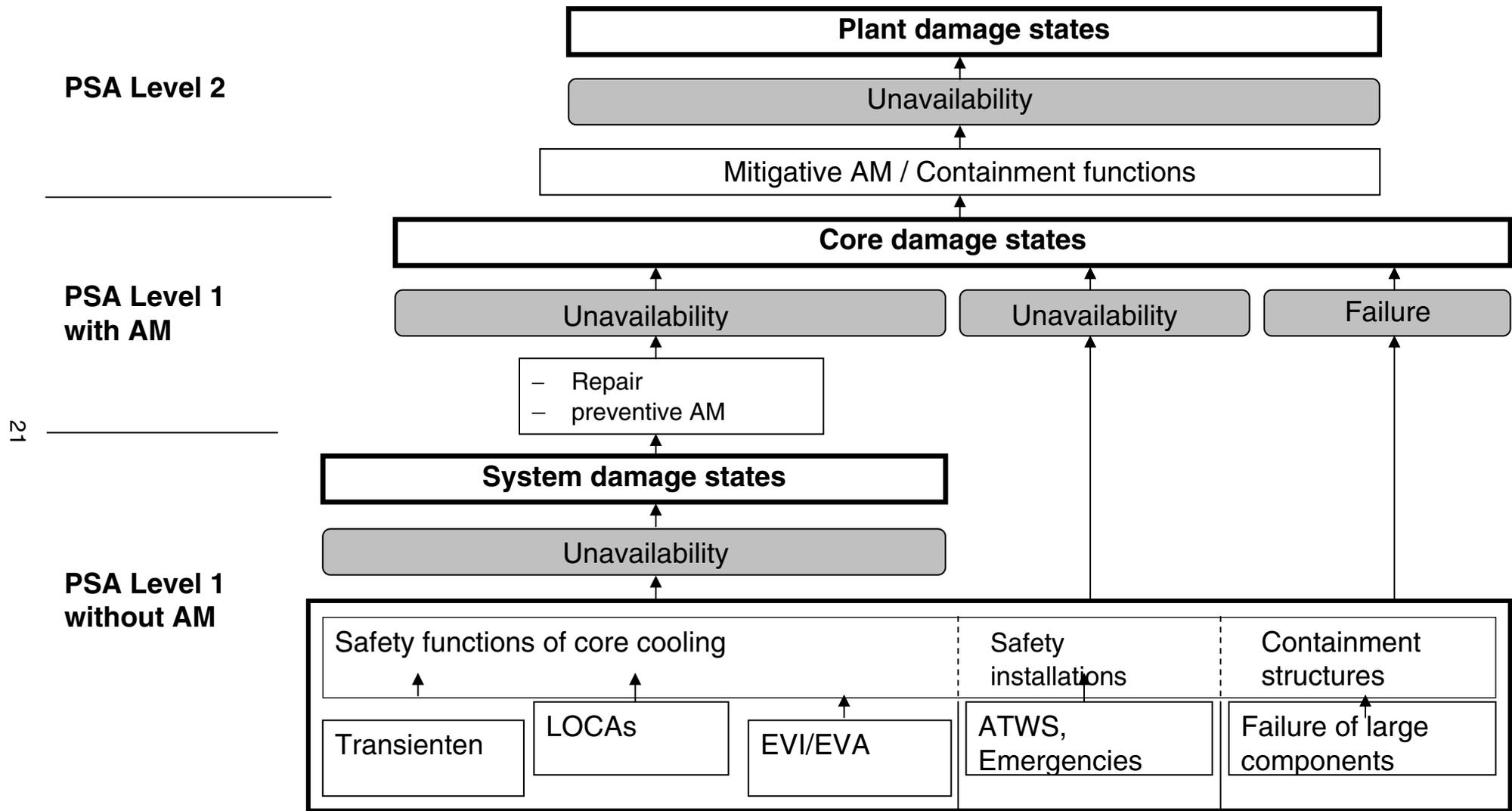
The level 2 of the PSA is to be based on a level 1, which is complete as far as possible and which is in compliance with the current state-of-the-art. Therefore, the PSA provided to GRS by the operator of GKN 2 NPP /GRS 01/ – in the following designated as Basis-PSA – has been modified according to the PSA standards of GRS, and its scope has been extended.

The Basis-PSA was in compliance with the German PSA Guideline /FAK 97/. However, the Guideline in a number of instances is ambiguous with respect to the methods to be applied. Furthermore, recent developments are not fully reflected in the Guideline.

For the present PSA GRS has applied methods considered as complying with the current state-of-the-art. In most instances these methods are in accordance with the German PSA Guideline, but they are advanced in important points. Particularly, the PSA Guideline does not comprise requirements for a low-power & shutdown PSA and for the level 2 of a PSA.

The adaptation of the Basis-PSA concerns mainly the following points:

- The evaluation of common cause failures (CCF) has been completely renewed (CCF model, CCF data).
- The fault tree analyses for important systems and the event tree analyses for the plant internal area events flooding and fire have been complemented or modified.
- Analyses for low power & shut-down states have been added.
- Different from the former practice, the results of the present PSA are not been presented in the form of point values, which have been calculated from the mean values of the input parameters. Instead, for all fault tree and event tree evaluations uncertainty analyses have been performed, delivering subjective probability distributions for all results.



21

Fig. 4.1 Scope of the PSA for a PWR with GKN 2 as reference plant

AM Accident Management
 ATWS Anticipated transients with failure to scram
 EVA external area events
 EVI internal area events

4 PSA approach

- The uncertainty of failure probabilities is described by means of Beta-distributions. In future PSA the uncertainty of failure rates will be described by means of Gamma-distributions. This modification has not been realized in the present PSA.
- The risk influences from an air-plane crash and from other external events and from a failure of large components with high energy content have been estimated.
- In the level 1 part of the PSA also procedures of the symptom oriented operating manual and of preventive plant internal accident management have been taken into account.
- The influence of recovery actions after accident initiation has been investigated for one example.
- An interface for the transfer of information from level 1 to level 2 of the PSA has been developed.
- For the level 2 part proven methods have been applied (EVENTRE for the event tree analysis, MELCOR for the accident simulation). However, the event tree analysis has been modified in such a way, that event sequences in level 2 can be traced back into level 1. Based on this approach, the event sequences dominating with respect to frequencies and consequences have been identified. In level 2 mitigating plant internal accident management has been taken into account.

Acts of terrorism and sabotage have not been considered in the PSA. Such risks are practically not accessible for a quantification. There is no basis for a sound evaluation of the expected frequency of willful detrimental acts of different kind and severity. A probabilistic evaluation of the plant vulnerability, achieving more than a more or less qualitative weak point analysis, would require methods – not available up to now – to evaluate probabilistically, among other things, the “expert knowledge” and the criminal intensity of aggressors. Furthermore it would not be justified to describe in a published document details of countermeasures – and potential ways to overcome them.

4.3 Characteristics of the “Basis-PSA”

Siemens-KWU (now Framatome ANP GmbH) on behalf of the plant operator has performed a PSA for GKN-2 NPP complying with the German PSA Guideline /FAK 97/ as

part of the Periodical Safety Review /SIE 98/. This PSA is called "Basis-PSA" in the current report.

In compliance with the PSA Guideline the Basis-PSA did investigate plant internal initiating events starting from normal power operation and took into account active containment functions.

The analysis comprises the identification of event sequences which are not kept under control by operational and safety systems (system damage states) and the calculation of frequencies of such event sequences. The analysis took into account event orientated operator actions planned in the operators manual to cope with accidents. Protective goal orientated actions, which also are planned in the operators manual, have not been quantitatively evaluated in the Basis-PSA.

Plant internal accident management, which can prevent system damage states to develop into a core damage, have been investigated for the "secondary side bleed and feed" only.

The reliability analyses have been performed with and without consideration of common cause failures (CCF) of redundant components in order to identify the influence of CCF on the PSA results. In the Basis-PSA CCFs have been analyzed and quantified by means of the SRA-model /FAK 97/ developed by Siemens-KWU.

Repair of failed safety relevant components after accident initiation has not been considered in the Basis-PSA.

The Basis-PSA has used a generic set of component reliability data for the quantitative evaluation of event trees and fault trees.

The Basis-PSA has evaluated the following leaks in the primary system:

- small leaks at a main coolant line (various diameters),
- medium leak at a main coolant line,
- leak at the pressurizer via a stuck open safety valve,

and LOCAs with a potential loss of the containment function because of a by-pass:

4 PSA approach

- steam generator tube rupture (double-ended break of one or two tubes)
- interfacing systems LOCA.

Detailed analyses have been performed for the "operational transients"

- loss of preferred power,
- loss of main feedwater,
- loss of main heat sink,
- loss off main feed water and loss of main heat sink,

and for the "unlikely transients"

- steam line break beyond the outer isolation valve,
- feedwater line break ahead of the pump shut-off valve.

The initiating events

- large leak at a main coolant line,
- leaks at the pressurizer caused by transients,
- steam line breaks and feedwater line breaks inside the containment,
- ATWS (anticipated transients without scram)

have not been analyzed in detail. Their contribution has been estimated.

As an example for "plant internal flooding" a

- leak in the fire-fighting system inside the reactor building annulus

has been analyzed.

The Basis-PSA found an expected frequency of system damage states of $1.5 \cdot 10^{-6}$ /a. If CCFs are not taken into account a value of $3.9 \cdot 10^{-7}$ /a is calculated. This means that 75 % of the system damage state frequency are caused by CCF. These figures are point values calculated with the mean values of the component reliability data.

If plant internal accident management is not effective, system damage states progress into a core damage state. The frequency of such events is $9.8 \cdot 10^{-7}$ /a.

In the Basis-PSA uncertainties of results have been analyzed. Because of restrictions of the used PSA program (“Risk Spectrum”) dependencies of epistemic uncertainties of the reliability data could be considered only for component failures with identical failure rates or failure probabilities. Furthermore, the uncertainty analysis of the Basis-PSA is based on approximations of the average unavailabilities of failure combinations (“minimal cuts”).

4.4 Modifications of the Basis-PSA

GRS has modified the Basis-PSA performed by Siemens-KWU. The modifications of the applied PSA methods are related mainly to the following points:

4.4.1 New evaluation of the influences from common cause failures (CCF) of redundant components

The Basis-PSA applied the SRA model developed by Siemens-KWU for the evaluation of common cause failures. GRS takes the view that this model is not appropriate to model in a satisfactory manner the operational experiences with CCFs and the insights concerning CCF phenomena. Therefore for the present PSA the SRA model has been replaced by a improved version – called Coupling Model – of the Binomial Failure Rate (BFR) Model which has already been used in the DRS-B. In the coupling model (/KRE 97/, KRE 98/) the fixed coupling parameters, formerly being used to evaluate an observed CCF event, have been replaced by an expert judgement of the degree of degradation of each component in the component group affected by the CCF event. The degree of degradation is evaluated according to a given scale used for the international CCF data exchange project ICDE /NEA 00/ resp. used by the USNRC /NRC 98/.

For the GKN-2 PSA the coupling model has been modified in such a way that the evaluation of the observed CCF events by several experts can be considered. By combining the individual distributions of the coupling parameters from each single expert evaluation, a common distribution is generated, which takes into account the different expert evaluations proportionally. In this way uncertainties of the judgement of CCF probabilities are implicitly taken into account.

4 PSA approach

By considering the different expert judgements for the transferability of a CCF event also the uncertainty of the evaluation of the transferability can be quantified. For this purpose the expert judgements are used to generate a distribution of the transferability parameter, which is used instead of the fixed factor in the old model.

All CCF events, which have been evaluated for the formerly used CCF data sets, have been newly evaluated according to the requirements of the new model. For the new evaluation also those CCF events have been considered, which have been evaluated by GRS in various projects since DRS-B.

4.4.2 Consideration of plant internal accident management

In former projects GRS has improved methods for the probabilistic evaluation of plant internal accident management (/PRE 98/, /BER 98/) in various important points. The improved methods have been applied in the present PSA for the evaluation of the accident management measures “secondary side bleed and feed (SBF)” and “primary side bleed and feed (PBF)”. The Basis-PSA did consider only the influence of the “secondary side bleed and feed”.

4.4.3 Consideration of repair of failed components

The present PSA considers to a limited extent the influence of repair of components, which are not available at initiation of an accident or which fail during an accident, on the potential to cope with an accident. The PSA considers recovery measures, which may be relevant for the PSA results and which meet the following conditions:

- Repair can be accomplished within a few hours by the organizational unit in charge.
- The probability for a successful repair is dominated by rule based operator actions.
- The conditions for a successful repair are met (e.g., identification of the failed component, availability of resources, accessibility of the component).

The present PSA investigated the possibility and the probability of a repair of failed components for the feedwater supply of the steam generators, before the accident management measure “primary side bleed and feed” has to be initiated (at a water level < min 3 in the reactor pressure vessel).

In the Basis-PSA, corresponding to the German PSA Guideline, repair has not been considered. The PSA Guideline requires that repair has to be considered only if prescribed by written instructions.

4.4.4 Evaluation of plant specific component reliability data

The Basis-PSA uses a generic set of component reliability data. The uncertainties of the data are described by lognormal distributions. For the present PSA plant specific data have been generated based on four years (1994 – 1997) of operational experience.

For components with only few events in the relatively short observation period of four years in GKN-2, generic data from other PWR plants, investigated by GRS, have been included into the evaluation. Dependent on the available information two different mathematical approaches have been used for the evaluation of the reliability data. For components with a sufficient number of events in GKN-2 the non-informative Bayesian approach has been used. If generic data had to be used to support the plant specific experience, these data were combined with the plant specific data as a-priori information for the superpopulation approach of Bayes (/HOF 99/, HOF 99a/).

The epistemic uncertainties on the true values of the reliability data are described by probability distribution types, which for mathematical reasons are most appropriate for the respective kind of data:

- For the frequencies of operational transients Gamma-distributions are used.
- For the frequency of leaks lognormal distributions are used.
- For important failure probabilities the uncertainties are described by Beta-distributions.

The uncertainties of component failure rates are still described – as in former PSAs – by lognormal distributions. In future PSAs they will be replaced by Gamma-distributions.

4.4.5 Modification of event tree and fault tree analyses

The event tree and fault tree analyses of the Basis-PSA have been modified in numerous points. In some cases additional thermohydraulic analyses have been performed and success criteria have been modified. The fault tree analyses consider additional CCFs and – different from the Basis-PSA – also operator actions planned in the protection goal oriented part of the operators manual.

The uncertainties of the results have been analyzed by means of a simulative approach, taking into account knowledge dependencies of initiating event frequencies, component reliabilities and operator action reliabilities (/GRS 90/). Knowledge dependency has been assumed for components, whose operational experience has been pooled for the evaluation of reliability data. In the Basis-PSA knowledge dependency of reliability data has been assumed only for component failures with the same failure rates or failure probabilities. Furthermore, the uncertainty analysis in the Basis-PSA uses only approximations of the average unavailabilities of the failure combinations (“minimal cuts”).

In the present PSA the influence (importance) of individual system functions, component failures and defined groups of component failures on the frequency of damage states has been calculated on the basis of mean values of the system functions (taken from the uncertainty analysis). In the Basis-PSA the importances have been calculated from the point values of the unavailabilities..

For the extension of the PSA into level 2 an interface has been generated, which transfers the information on core damage states into the level 2 analyses.

4.4.6 Evaluation of probability distributions and mean values

In a late phase of the work for the present PSA it turned out that the formerly used approach for the consideration of data uncertainties is unsatisfactory.

It was common practice, first to calculate “point values” of the PSA results and to use for this purpose the mean values of component reliability data as “point values” for the input parameters. Afterwards probability distributions of the bottom line results have been calculated from the probability distributions of the input parameter. This approach

requires much less analytical effort than a continuous consideration of the probability distributions.

Although point values are calculated from the mean values of the input parameters, they are more or less different from the mean values of the probability distributions of the results. These differences are caused by the "failure rate coupling". If reliability parameters for several components are based on the same source of information, they are not drawn independently for the uncertainty analysis, but the same ("coupled") value is used for all of these components. For the calculation of point values failure rate coupling is not taken into account.

In the present PSA surprisingly large differences between point values and the mean values of contributors to the frequencies of system and core damage states have been found. From this fact it has been concluded, that point values should only be used for a first orientation about the PSA results.

In the present PSA the analytical results are no longer presented in the form of point values, which have been calculated from the mean values of the input parameters. Instead, for all fault tree and event tree evaluations uncertainty analyses have been performed, generating subjective probability distributions for all results. This modification of the basic method, which was realized in a late phase of the study, required considerable additional effort and caused several months of delay for the completion of the study.

4.4.7 Events during low power and shutdown states

The PSA has been extended to events during low power and shut-down states. Specific methodical problems of this part of the PSA are discussed in chapter 7.

4.5 Extension of the PSA by fire analyses

4.5.1 Selection of fire risk relevant areas (Screening)

It is international practice and required also in the German PSA Guideline, to identify in a first step fire risk relevant areas, in order to reduce the effort for in-depth analyses

4 PSA approach

(screening). Our investigations have shown, however, that the methods described in the PSA Guideline are not appropriate to meet the goals of the screening process.

This is proven by the fact, that 137 out of 271 room areas in the reactor building annular room meet the qualitative criteria formulated in the PSA Guideline. Also the second (quantitative) screening process described in the PSA Guideline, based on the Berry approach, is hardly practicable, because the selection criteria require information on resulting core damage states, which is not available at this point of investigation and which could only be gained by extensive investigations.

In a research project GRS has developed a new practicable approach (/FAS 01/). This approach has been applied in the present PSA. The approach comprises a systematic and unified preparation of information, an immediate combination of qualitative and quantitative criteria applying elements of the Berry approach and a final expert judgement. This approach has proven to be practicable and is recommended for future fire PSAs.

4.5.2 Frequency of fires

The method described in the PSA Guideline to evaluate the frequency of fires - based on the Berry approach – has proven to be principally appropriate. The method starts from statistically evaluated generic frequencies of fires in a building and splits these frequencies into individual room areas, taking into account plant specific situations. In order to verify this "top down" approach we have additionally used a "bottom up" approach, which evaluates fire frequencies by means of specific fault tree analyses. The values calculated for a practical example are in good agreement. However, mainly the "top down" approach requires an improved data basis. Related work is going on in a research project at GRS applying also data from French nuclear power plants.

4.5.3 Evaluation of fire consequences

For the evaluation of fire consequences by an in-depth analysis it is generally accepted to apply simplified simulation models, as far as simple room geometries and ventilation conditions are to be analyzed. We have investigated, whether verified realistic results can be gained by means of the currently available zone models also for more complicated situations and conditions than prevailing in the reactor building. For this purpose

various fire simulation models have been used and comprehensive uncertainty and sensitivity analyses have been performed. The results show, that the multi compartment-/ multi zone-model CFAST generally calculates higher fire room temperatures than the system code COCSYS. The differences are caused by the considerably simplified modeling of the room geometry in the zone model. The finding is, that – according to the results of the simulation – smaller amounts of hot gases will flow into higher areas of the building and that less cold air is added. The most important insight from the uncertainty analysis is that code-immanent uncertainties are dominating. The results of these analyses also show, that the variation of the temporal dependencies of important parameters should be given more importance in future uncertainty analyses. Overall it can be concluded that sophisticated zone models, as they are available now, will produce reliable results also for complicated constructional situations. Exceptionally unrealistic results can be recognized and evaluated by means of appropriate nodalisation, by comparing results from diverse simulation codes and by including the know-how of experts.

4.5.4 Event tree and fault tree analyses

At the current state of PSA methodology the investigation of fire specific event sequences with respect to fire fighting and fire control applies event tree and fault tree analyses. This approach has produced reliable and appropriate results also with respect to the quantification of uncertainties. In an actual research project GRS has developed an alternative approach for a simulative fire fighting model. This model has been used in the present PSA for an additional uncertainty and sensitivity analysis. However, the results of these calculations have not been available prior to the completion of the PSA.

4.5.5 Fire effects on the technological systems

The insertion of component failures caused by fires into existing fault trees for initiating events investigated in the PSA – as described in the PSA Guideline – is very difficult in some cases or even impossible. Even if the fire scenario investigated can be associated with certain transients (loss of main coolant pump, reactor scram, disturbance of feed water supply to a steam generator), the possibility of a simultaneous or a staggered occurrence of these transients makes the evaluation difficult. Applying the currently available fire simulation models the point of time of transient initiation by a fire-

4 PSA approach

induced cable failure can be evaluated only very coarse, even if more detailed information on the function of affected cables and their localization would be available than we had for the present PSA.

Up to now it is not evident, how the various possibilities of fire induced failures of I & C cables (break, signal alteration, overvoltage) and their different consequences can be considered in a PSA. The consequences of the cable fire investigated in the PSA on the I & C system were mainly related to operational measured values and limit values of the reactor protection system. If in the extreme case a fire spreads over two redundancies, a simultaneous occurrence of faulty signals in two redundancies of the data acquisition with the possible consequence of faulty actions of the reactor protection system has to be considered. The analysis and evaluation of such failures requires improved methods. These problems should be taken into account for the further development of PSA methods.

4.5.6 Summary of the results of the fire analysis

The investigations in this PSA do not comprise a complete fire PSA. Only one room area was investigated in detail, which however is representative for possible fires inside the containment in the reference plant.

By the screening process for the identification of fire relevant room areas further rooms have been found, which should be investigated in a complete fire PSA in order to estimate their contributions to the frequency of system and core damage states. For the annular room of the reactor building, e.g., about eight room areas should be investigated in detail according to the results of the screening process. For the switchgear building, the emergency diesel building, and the emergency feedwater building the screening has not been performed up to now.

In order to estimate the relevance of fire events for the frequency of system and core damage states calculated in the level 1 PSA it has to be considered that many of the still to be investigated room areas are representative for further rooms with respect to the frequency of occurrence and possible consequences and that a great number of single contributions have to be summed up in order to get the overall contribution of fire events. Even if the individual contributions are small, which is to be expected because of the modern fire protection design of the reference plant, the overall contribution of

fire events could sum up to frequencies of system and core damage states, which are in the region of contributions from other initiating events.

5 Level 1 PSA for power operation

5.1 Initiating Events

In the first step of the PSA, initiating events have to be identified, which lead to a failure of operational systems for core cooling and heat removal, so that the intervention of systems with safety function is required to maintain a sufficient heat removal from the reactor core. The safety functions are carried out by safety systems supported by operational systems and emergency systems (in German: "Notstandssysteme"). Therefore, in the following, safety functions are denoted more generally as "system functions". Initiating events can be caused by component malfunctions and damages, by plant internal hazards (e.g. fire, internal flooding), or by external hazards (e.g. earthquake).

For all initiating events occurrence frequencies have to be evaluated. In part these frequencies can be derived directly from operating experience. If an initiating event has not yet occurred, the estimated frequency is only determined by the observation period (zero failure statistics). In case of relatively short observation periods this can lead to a significant overestimation of the real frequency. The PSA applies the following methods in order to obtain realistic estimations:

- The initiating event (e.g. "pressurizer leak caused by transients") results from a triggering event, for which the frequency can be directly derived from the operating experience (in the example "opening of the pressurizer valve in case of transients"). The probability of an initiating event as a consequence of the triggering event (in the example "valve fails to close and failure of the isolation") is estimated by a fault tree analysis.
- The initiating event frequency (e.g. "small leak at a main coolant line, 25 - 80 cm²") is derived from the operating experience in combination with model assumptions.

The initiating events investigated in this PSA and their frequencies are described in section 5.1.1 and listed in table 5.1.

Table 5.1 Initiating event frequencies

No.	Designation of the event group Designation of the event	frequency [1/a]
Leak in the pressure boundary of the primary system inside the containment		
1	Large and medium leak at a main coolant line, > 200 cm ²	< 1E-7
2	Small leak at a main coolant line, 80 - 200 cm ²	9.0E-5
3	Small leak at a main coolant line, 25 - 80 cm ²	1.5E-4
4	Small leak at a main coolant line, 2 - 25 cm ²	3.0E-3
Leaks at the pressurizer		
5	Small leak at the pressurizer caused by transients, 20 cm ²	4.1E-6
6	Small leak at the pressurizer by stuck open safety valve, 40 cm ²	8.5E-4
7	Interfacing systems loss of coolant accident	< 1E-8
Steam generator tube rupture		
8	Leak 1 - 6 cm ²	2.3E-3
9	Leak 6 - 12 cm ²	1.0E-5
Operational transients		
10	Loss of preferred power	2.5E-2
11	Loss of main feedwater without loss of main heat sink	1.2E-1
12	Loss of main heat sink without loss of main feedwater	3.8E-2
13	Loss of main feedwater and loss of main heat sink	7.5E-3
Transients caused by steam generator overfeeding and main steam line or feedwater line breaks		
14	Steam generator overfeeding	1.0E-5
15	Main steam line break outside the containment	1.6E-4
16	Main steam line break inside the containment	< 1E-7
17	Feedwater line break outside the containment	2.6E-4
18	Feedwater line break inside the containment	< 1E-7
Anticipated transients without scram (ATWS)		
19	ATWS in case of loss of preferred power	< 2E-8
20	ATWS in case of loss of main feedwater	< 1E-7
21	ATWS in case of loss of main feedwater and loss of main heat sink	< 7E-9
22	ATWS in case of other transients	< 5E-8
Transients caused by internal hazards		
23	Transient caused by a leak in the fire extinguishing system inside the annulus	< 3.0E-7
24	Transients caused by fire inside the containment	1.8 E-5

For those initiating events, which have been attributed to triggering events, table 5.2 contains the frequencies of the triggering events, the probabilities for the failures of countermeasures under the assumption that the triggering event did occur and the resulting frequencies of the initiating events.

The estimations for those events, which have not been further investigated due to their low importance for the core damage states and for the level 2 of the PSA, are described in section 5.1.2.

In order to facilitate the understanding of the further tables, they are endowed with the following picture in reduced size. In each case the arrow is marked which indicates the contents of the respective table (transition from triggering events to initiating events, transition from initiating events to damage states, transition between damage states) is highlighted. The terms “system damages state“, “core damage state“ and “plant damage state“ are defined later in the text.

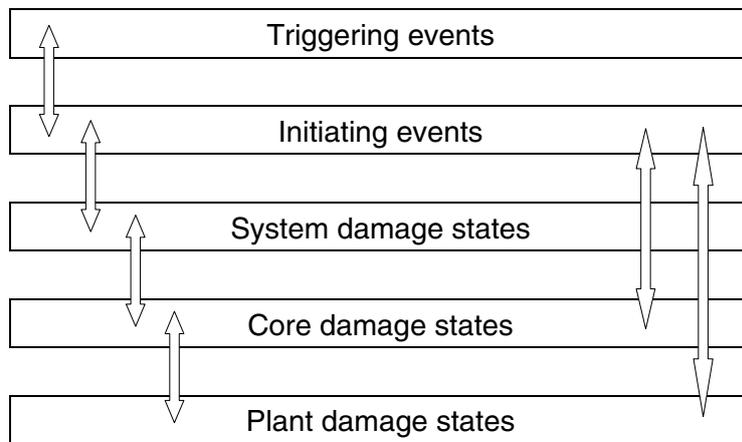


Table 5.2 Frequencies of triggering events and probabilities for the transition from

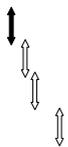
Triggering event		Transition
Designation	f [1/a]	Relevant system function
Opening of the pressurizer relief valve during transients	7.5E-3	failure to close and failure of the isolation measure
Inadvertent opening of a pressurizer safety valve	2.0E-2	failure to close
Leak in the injection line of the volume control system	3.4E-3	failure of the isolation measure
Operational steam generator overfeeding with demand of overfeeding protection by RP signals	2.3E-2	failure of overfeeding protection by RP signals
Loss of preferred power	2.5E-2	failure of scram
Loss of main feedwater	1.2E-1	failure of scram
Loss of main feedwater and loss of main heat sink	7.5E-3	failure of scram
Other transients	5.0E-2	failure of scram
Leak in the fire extinguishing system inside the annulus	3.0E-5	Failure of measures for leak limitation
Pilot fire at a cable distribution inside the containment	9.2E-5	Failure of fire protection measures

1) see table 5.1
 p probability
 RP reactor protection

f frequency
 ATWS anticipated transient without scram
 SG steam generator

triggering events to initiating events

probability p	Initiating event		f [1/a]	No. ¹⁾
	Designation			
5.5E-4	Small leak at the pressurizer induced by transients		4.1E-6	5
4.2E-2	Small leak at the pressurizer by stuck open safety valve		8.5E-4	6
< E-7	Interfacing system loss of coolant accident		< 1E-8	7
4.4E-4	Steam generator overfeeding		1.0E-5	14
< 9.0E-7	ATWS in case of loss of preferred power		< 2E-8	19
< 9.0E-7	ATWS in case of loss of main feedwater		< 1E-7	20
< 9.0E-7	ATWS in case of loss of main feedwater and of main heat sink		< 7E-9	21
< 9.0E-7	ATWS in case of other transients		< 5E-8	22
1.0E-2	Transient caused by a leak in the fire extinguishing system inside the annulus		< 3.0E-7	23
2.0E-1	Transients caused by a cable fire inside reactor building		1.8E-5	24



5.1.1 Investigated initiating events and their frequencies

In table 5.1 the initiating events investigated in this PSA and their frequencies are listed. The altogether 24 initiating events are assigned to 8 groups.

- **Leaks in the pressure boundary of the primary system inside the containment**

This group contains all leaks in the main coolant line, in connected lines until the isolation valves and leaks at the main coolant pumps. Leaks in the pressurizer vessel, in the inlet or outlet chamber of a steam generator and small leaks at the reactor pressure vessel are treated like a leak at a main coolant line. Large leaks in the reactor pressure vessel can be excluded due to the extremely high quality of the vessel.

In case of initiating events of this group, the coolant discharged from the leak is collected in the bottom of the containment (reactor building sump) and is available for core cooling.

The frequencies of "leaks at a main coolant line" have been taken from the German Risk Study, Phase B /GRS 90/. The relatively high effort for a re-evaluation of the operating experience did not seem to be justified, because essential differences from the estimates of the German Risk Study, Phase B were not to be expected /BEL 99/.

Considering the different success criteria for the system functions necessary to cope with main coolant line leaks, the following groups of leak sizes are distinguished:

- Large leak $> 500 \text{ cm}^2$
- Medium leak $200 - 500 \text{ cm}^2$
- Small leak
 - $80 - 200 \text{ cm}^2$
 - $25 - 80 \text{ cm}^2$
 - $2 - 25 \text{ cm}^2$

Leaks $< 2 \text{ cm}^2$ can be overfed by operational systems. Therefore they are not treated as initiating events.

The small leak 2 - 25 cm² is subdivided into a leak 2 - 12 cm² and a leak 12 - 25 cm² for the evaluation of system and core damage state frequencies (see sections 5.2.3 and 5.3.3.3)

The frequencies of a small leak 2 - 12 cm² at a main coolant line have been estimated in the German Risk Study, Phase B based on the operating experience /BEL 99/.

The frequencies of leaks > 12 cm² have been evaluated based on model considerations. Due to the high quality standard of the lines of the reactor coolant circuit leaks > 200 cm² at a main coolant line and at out-bound parts of connected lines can be practically excluded (frequency < 10⁻⁷/a, /BEL 99/). Large and medium leaks have been investigated conjointly because the influence of these leaks on the frequency of system and core damage states and on the results of the level 2 of the PSA is estimated to be small (see table 5.1 and section 5.1.2).

- **Pressurizer leaks**

Pressurizer leaks can occur if the pressurizer relief valve or a pressurizer safety valve opens as a consequence of transients or due to other reasons and faultily remains open and if (in case of a stuck open relief valve) the pressurizer relief stop valve does not close.

As with leaks at a primary coolant line inside the containment, the coolant discharged from the leak is collected in the bottom of the containment (building sump) and is available for core cooling.

The frequencies for "pressurizer leaks" result from:

- the frequency of the triggering events "opening of the relief valve in case of a transient" and "faulty opening of a safety valve" and
- the probability for the failure of countermeasures (closing of the faultily open valve resp. the pressurizer relief stop valve).

A turbine trip (TUSA) with a failure of the main steam bypass system (FDU) leads to an opening of the pressurizer relief valve in case of transients. In contrary, in case of transients with TUSA and a consequent blocking of the main steam bypass system (after being open for a short time period) the actuation pressure of the pressurizer relief valve

is only reached if, in addition, the operational coolant temperature control or the coolant pressure control or the reactor power limitation (LOOP-RELEB) or the partial shutdown fail.

The frequency of a transient with opening of the pressurizer relief valve was estimated based on the operating experience with nuclear power plants of the Pre-Konvoi and Konvoi type (zero failure statistics). During the observation period (starting with the beginning of commercial operation and ending on December 31, 1996) an opening of this valve was not observed during power operation. The probability for a failure to close the pressurizer relief valve and the pressurizer relief stop valve was evaluated by systems analysis.

The frequency of a pressurizer leak caused by stuck open safety valve was taken from the German Risk Study, Phase B. There the frequency was evaluated from operating experience. The failure probability of the isolation measure was evaluated by systems analysis.

- **Leaks at the primary circuit within the annulus**

In case of non-isolable leaks in lines connected to the reactor cooling circuit outside the containment a loss of primary coolant occurs, and consequential failures of safety related equipment within the reactor annulus are possible.

In case of a primary circuit leak within the annulus the leaking water is not collected in the reactor sump. Therefore, it is not available for core cooling. Furthermore, fission products can be released into the environment, by-passing the containment.

The frequency of a non-isolable primary circuit leak within the reactor building annulus is evaluated from the frequency of the triggering events, derived from operating experience, and the probabilities for the failure of the isolation measures by means of systems analysis. The frequencies of leaks at the lines connected to the reactor coolant system have been taken from the German Risk Study, Phase B /GRS 90/.

- **Leaks at steam generator tubes**

Via a leak at a steam generator tube, primary coolant flows from the primary reactor circuit (which is under higher pressure) into the feedwater steam circuit. Considering the different success criteria for the system functions to cope with leaks at steam generator tubes, two leak sizes are distinguished (1 - 6 cm² and 6 - 12 cm²).

Because in case of a leak at steam generator tubes the leaking water is not collected in the containment sump, and is, therefore, not available for core cooling. Furthermore, fission products can be released into the environment, by-passing the containment.

The frequencies for leaks at steam generator tubes for leak cross sections up to the double cross section of one tube ($\leq 6 \text{ cm}^2$) are derived from the operating experience of German nuclear power plants and of the nuclear power plants Borssele, Gösgen and Trillo built by KWU (zero failure statistics). For leak sizes of 6 - 12 cm² the frequency is adopted from the German Risk Study, Phase B. The basic assumptions and model perceptions applied there to evaluate the leak frequency comply with the current knowledge of steam generator tube leaks /BEL 99/.

- **Anticipated transients**

Transients are events disturbing the heat removal from the reactor core without loss of coolant. "Anticipated transients" are transients which with high probability are expected to occur during the life time of a nuclear power plant. In this group the following events have been investigated:

- Loss of preferred power (loss of auxiliary power supply)
A loss of preferred power causes a loss of the main feedwater supply of the steam generators, of the turbine condenser as main heat sink and of the main coolant pumps.
- Loss of main feedwater supply without loss of the main heat sink
- Loss of the main heat sink without loss of main feedwater supply
- Loss of main feedwater supply and of the main heat sink

The results for the frequencies of system and core damages states and for the level 2 of the PSA from these initiating events include also the contributions from anticipated transients which are triggering events for these initiating events (e.g. loss of a main

feedwater pump). Contributions from other anticipated transients (e.g. loss of main coolant pumps) are estimated to be not relevant for the results.

The frequencies of anticipated transients have been evaluated from the operating experience of Konvoi- and pre-Konvoi-plants. In case of loss of preferred power also the operating experience with other German PWR and BWR plants was applied to evaluate the frequency. The design of the auxiliary power supply is important for the frequency of a loss of preferred power. Today, all German NPPs have two external AC power supplies and the internal AC power supply from the main generator. Therefore, they are equivalent with respect to the frequency of a loss of preferred power.

- **Transients caused by steam generator overfeeding and main steam line or main feedwater line breaks**

- Steam generator overfeeding

In case of overfeeding of a steam generator with the intrusion of feedwater into the main steam line a consequential damage of the main steam line may occur. The frequency of a steam generator overfeeding is evaluated from the triggering event "operational steam generator overfeeding with the demand of overfeeding protection by the reactor protection system" and the probability for a failure of the overfeeding protection (reactor protection system). The frequency of the triggering event was estimated from the operating experience with Konvoi- and pre-Konvoi-plants. The probability for the failure of the overfeeding protection is based on systems analysis.

- Main steam line or main feedwater line breaks

The PSA investigates the break of a main steam line and the break of a main feedwater line outside the containment. The frequencies of a break of a main steam line resp. of a main feedwater line are based on the evaluation of the operating experience with nuclear power plants of Western design /BEL 99/.

- **Anticipated transients without scram (ATWS)**

The following four cases are distinguished for anticipated transients without scram:

- ATWS in case of loss of preferred power
- ATWS in case of loss of main feedwater

- ATWS in case of loss of main feedwater and loss of main heat sink
- ATWS in case of other anticipated transients

The ATWS frequencies result from the frequencies of the triggering events (anticipated transients) and the failure probability of the reactor scram. The frequencies of anticipated transients result from the operating experience with Konvoi- and pre-Konvoi-plants resp. from all German nuclear power plants (loss of preferred power). The failure probability for a scram was estimated by systems analysis based on the national and international operating experience.

- **Transients caused by plant internal area events**

This group contains transients caused by:

- flooding of the reactor building annulus caused by a leak of the fire extinguishing system SGB and by
- cable fire inside the containment.

- **Flooding**

In case of a leak at the fire extinguishing system SGB inside the annulus safety relevant components in this room are flooded if leak-limiting measures fail. The failure, caused by flooding, of transducers or pumps inside the annulus can trigger a transient. The investigated leak at the fire extinguishing system SGB inside the annulus can occur in one of the two parts of the line, each between the inlet into the annulus and an isolation valve, which is closed during normal power operation. This is the most unfavorable leak location with respect to flooding of the reactor annulus. The fire extinguishing system has the highest potential with regard to the amount of water discharged into the annulus. Flooding of the reactor annulus by water from other systems or flooding of other buildings is assessed to be negligible in comparison.

The frequency of the triggering event "leak at the fire extinguishing system inside the reactor building annulus" is evaluated from the worldwide operating experience. The failure probability of measures limiting the leak discharge was estimated by means of a systems analysis. Personnel actions are needed in order to isolate the leak. The failure of these personnel actions is essential for the probability of an isolation failure. A failure probability of $p = 1 \cdot 10^{-2}$ was estimated by a screening analysis applying the ASEP

method /FAK 97/. This probability is dominated by the failure of isolation measures. A failure of leak detection is assessed to be essentially less probable (approx. $1 \cdot 10^{-3}$). Due to the approach of the assessment the estimated probability can be seen as a pessimistic upper estimate. Furthermore, the estimate is based on pessimistic boundary conditions with respect to the time periods available for isolation measures. As an upper estimate, the measures limiting the leaks are assumed to be failed if the water in the reactor annulus exceeds a level of 64 cm. This is the installation level of the extra boring pumps (lower edge of the motor), which are assumed to fail as a consequence of the flooding. An additional water release can trigger a transient caused by a consequential failure of the component cooling pumps located inside the reactor annulus. In this case, also the consequential failure of the residual heat removal pumps located on a lower level has to be assumed. In the present PSA it was not possible to analyze transients caused by faulty signals as a consequence of a flooding induced failure of transducers inside the reactor annulus.

- **Cable fires**

A cable fire inside the reactor containment was analyzed in detail as representative for fires affecting more than one redundant train. Redundant safety installations inside the containment are in most cases not separated by building structures, but only by space. This plant region therefore is of particular interest with respect to fire propagation. Furthermore, for a level 2 PSA particularly those areas are relevant, for which a fire does not only trigger an initiating event, but may also impair the integrity of the containment. Only cable fires close to the containment or to its isolation armatures have such a potential. Due to the plant specific conditions it seemed advisable to analyze a fire in the area of the cable penetrations inside the containment in order to allow the assessment of the impacts on the containment wall. Moreover, the possibilities of manual fire fighting by the fire brigade in case of a fire inside the containment are estimated by fire safety experts to be in part very limited. This also concerns the consideration and assessment of such fire protection means in the PSA. For clarification knowledge on the possible local and global temperature time histories in case of fires inside the containment is necessary, which could be gained by the analysis performed.

The probabilistic assessments are related to the evaluation of the frequency ($9.2 \cdot 10^{-5}/a$) of the triggering event (pilot fire at a cable distribution of one redundant train inside the containment) and of the frequency of the initiating event, considering possible fire se-

quences and the unavailability of fire protection measures. Transients (loss of a main coolant pump, malfunctions of the feedwater supply to a steam generator) have been estimated to occur with a frequency of $1.8 \cdot 10^{-5}/a$ as initiating events triggered by fire.

5.1.2 Estimations for initiating events not investigated in detail

In the present PSA initiating events are not analyzed in detail, if their influence on the results for core damages states and for the level 2 of the PSA is negligible or if a reliable method for a detailed assessment is not available. The potential contributions of these initiating events to the core damage frequencies are estimated in sections 5.1.2.1 to 5.1.2.3.

The initiating events treated in section 5.1.1 and in this section cover a representative spectrum of initiating events, which is sufficient to assess the accidental risk of modern pressurized water reactors (PWR) in Germany. We do not expect significant additional contributions to the core damage frequencies resp. to the frequencies of radioactive releases from initiating events not considered in this PSA.

5.1.2.1 Loss of coolant accidents (LOCA)

- **Large and medium leak at a main coolant line ($> 200 \text{ cm}^2$)**

For large and medium leaks at a main coolant line with a leak cross section $> 200 \text{ cm}^2$ a frequency of $< 1 \cdot 10^{-7}/a$ was estimated (see table 5.1 in section 5.1.1). To cope with a large leak at a main coolant line (leak cross section $> 500 \text{ cm}^2$) requires low pressure injections with suction from the borated water storage tanks and by sump recirculation into both legs (hot and cold) of at least one intact circuit or into one injection leg (hot or cold) each of at least two intact circuits. In case of a medium leak ($200 - 500 \text{ cm}^2$) additionally at least one high pressure injection into the hot or cold leg of one intact circuit is required. For this reason, the minimum system function requirements are more unfavorable for the medium leak. The unavailability of the system functions required to cope with a medium leak at a main coolant line is estimated to approx. $1,5 \cdot 10^{-3}$ by means of an event tree and fault tree analysis. This leads to a negligible frequency for system damage states from large and medium leaks of $< 1 \cdot 10^{-9}/a$. Because of this low fre-

quency these leaks are also negligible for the frequency of the core damage states and for the level 2 of the PSA.

- **Small leak at the pressurizer induced by transients**

The frequency of a small leak at the pressurizer induced by transients is $4.1 \cdot 10^{-6}/a$ (see table 5.1 in section 5.1.1) and so it is much lower than the frequency of a small leak induced by a stuck open safety valve with $8.5 \cdot 10^{-4}/a$. Because the system functions required to cope with the leak and the accident sequences are essentially identical for both cases, the contribution of small leak at the pressurizer induced by transients to frequency of system damage states resp. core damage states can be neglected.

- **Leaks at a primary coolant line outside the containment**

For the triggering event "leak in the feed line of the volume control valves" a frequency of $3.4 \cdot 10^{-3}/a$ has been estimated. The probability for the failure of the isolation measures was evaluated to $2 \cdot 10^{-7}$ by means of a systems analysis. This results in a frequency of the initiating event "non-isolable leak in the injection line of the volume control valves into the reactor annulus" of $< 10^{-9}/a$. Similarly low frequencies have been estimated for non-isolable leaks at other lines connected to the reactor coolant system. In total, the frequency of a "leak at a primary coolant line outside the containment" is estimated to be $\ll 1 \cdot 10^{-8}/a$. Within the design basis system functions to cope with the initiating event are not available. In consequence, a non-isolable leak is equivalent to a system damage state. If accident management measures are not considered, the system damage state will progress into a core damage state. With the frequency of $\ll 1 \cdot 10^{-8}/a$ leaks at a primary coolant line outside the containment are negligible compared to the evaluated total core damage frequency. The influence on the results of the level 2 primarily pertain to the release category FKB /MEI 01/, the frequency of which would be increased by significantly less than 50 %. In contrast, the contribution of leaks at a primary coolant line outside the containment to the frequency of release category FKA with much higher radioactive releases would be negligible (< 1 %).

- **Steam generator tube leak, 6 - 12 cm²**

The frequency of a "steam generator tube leak, 6 - 12 cm²" is $1.0 \cdot 10^{-5}/a$, and so it is much lower than the frequency of a steam generator tube leak of size 1 - 6 cm² (see table 5.1). To cope with a steam generator tube leak, 6 - 12 cm², requires

- one high pressure injection into one of the four circuits,
- a secondary side partial cooldown or a long-term residual heat removal via one of the four steam generators, and
- the isolation of the damaged steam generator or a long-term residual heat removal via one of the four steam generators.

The unavailability of the system functions has been estimated to approx. $4,0 \cdot 10^{-4}$ by means of an event tree and fault tree analysis. This results in a frequency of approx. $4 \cdot 10^{-9}/a$ for system damage states in case of a steam generator tube leak, 6 - 12 cm², corresponding to about 2 % of the frequency of a system damage state in case of a steam generator tube leak, 1 - 6 cm² (see section 5.2.5). In case of steam generator tube leaks the probability for the success of accident management measures is estimated to be very low (see section 5.3.1.1). Therefore, for both cases of steam generator tube leaks the core damage frequency corresponds to the frequency of system damage states. Because the effects on radioactive releases are estimated not to be essentially different for both leak sizes, the steam generator tube leak, 6 - 12 cm² does not deliver significant contributions to the results of the level 2 of the PSA.

5.1.2.2 Transients induced by plant internal triggering events

- **Transient induced by steam generator overfeeding**

The frequency of a steam generator overfeeding with loss of the overfeeding protection by the reactor protection system is approx. $1 \cdot 10^{-5}/a$ (see tables 5.1 and 5.2 in section 5.1.1). If the main feedwater pumps are not switched off manually, large amounts of water flows into the main steam line with the risk of consequential damages in the main steam system. If - as an upper estimate - the switch-off failure and the break of a main steam line outside the containment are both assumed with a probability of 1, a frequency of $1 \cdot 10^{-5}/a$ is estimated as upper limit for the break of a main steam line as consequence of a steam generator overfeeding. With respect to the frequency of a main

steam line break, a consequential break of a main steam line induced by steam generator overfeeding is negligible in comparison to the initiating event "main steam line break outside the containment" (frequency $1.6 \cdot 10^{-4}/a$, see table 5.1). The unavailability of the system functions required to cope with a main steam line break outside the containment is similar for both cases. Therefore the steam generator overfeeding can also be neglected with respect to the frequency of system damage states. Because, furthermore, significant differences in the transition probabilities to a core damage state and with respect to the results of the level 2 of the PSA are not seen, a steam generator overfeeding is negligible in comparison to the initiating event "main steam line break outside the containment" (for a "main steam line break outside the containment" only the frequency of a system damage state has been evaluated, see section 5.2.13).

- **Transient induced by main steam line break inside the containment**

For the main steam lines inside the containment (between steam generator and main steam isolation valves) it was demonstrated that breaks can be practically excluded. Therefore the frequency of a main steam line break or a connected line break inside this area is estimated to be $< 1 \cdot 10^{-7}/a$. Because the leak is not isolable against the steam generator, only three - or in case of additional failures of main steam isolation valves (failure to close) less than three - steam generators are available for the secondary side heat removal. Based on calculations for the "main steam line break outside the containments" (see section 5.2.10) a value of $< 1 \cdot 10^{-2}$ is estimated for the unavailability of those system functions required to cope with a break inside the containment. This results in a system damage frequency of $< 1 \cdot 10^{-9}/a$, which is less than 1 % of the system damage frequency for the "main steam line break outside the containment" and, hence, assessed to be negligible. A main steam line break inside the containment contributes only marginally also to the total core damage frequency and it is assessed to be negligible with respect to its effects on the frequencies of radioactive releases.

- **Transients induced by a feedwater line break inside the containment**

As for the main steam lines also for the feedwater lines inside the containment break exclusion has been demonstrated. The frequency of feedwater line breaks is estimated to be $< 1 \cdot 10^{-7}/a$. It depends on the location of the leak, if the steam generator of the affected redundancy is available for the injection via the emergency feedwater system. The unavailability of the system functions required to cope with a feedwater line break

inside the containment is estimated to be $< 1 \cdot 10^{-2}$. This results in a frequency of system damage states of $< 1 \cdot 10^{-9}/a$. Without considering accident management measures the system damage states would progress into core damage states with a probability of 1. The contribution represents less than 1 % of the core damage frequency of the anticipated transients.

- **Anticipated transients without scram (ATWS)**

Anticipated transients without scram (ATWS) can be controlled by the moderator density feedback on the reactivity. This inherent safety mechanism reduces the power generated in the reactor core and limits the maximum pressures in the primary and secondary system. Calculations with the analysis simulator GKN 2 have shown that an ATWS can be controlled even in case of additional failures on the primary as well as on the secondary side. This is valid under the premise that at least two of the three pressurizer valves open and the secondary side heat removal is performed via the main steam by-pass station or via three out of four main steam release stations (relief or safety valve, resp.) and that at least one steam generator is fed /HÖP 00/. With the evaluated total frequency of ATWS cases of $< 1,7 \cdot 10^{-7}/a$ and a system unavailability of $< 1 \cdot 10^{-2}$ the contribution to system damage states with a value of $< 2 \cdot 10^{-9}/a$ is considered to be negligible. If for an upper estimate accident management measures are not taken into account, a core damage frequency of $< 2 \cdot 10^{-9}/a$ results which is also negligible. From estimations of the frequencies of radioactive releases in the individual release categories negligible contributions from ATWS are to be expected.

- **Transients induced by flooding of the reactor building annulus**

For a transient induced by flooding inside the reactor building annulus a frequency of $< 3,0 \cdot 10^{-7}/a$ was evaluated. The transient can be caused by a consequential failure of the pumps, among others, of the nuclear component cooling water system. In this case, also a consequential failure of the extra borating and RHR pumps located on a lower level has to be assumed. The heat removal from the reactor cooling circuit via the steam generators is not affected in these cases.

For estimating the transition probabilities from the initiating event to a system damage and core damage state it is distinguished between detected leaks and not detected leaks as triggering events. The corresponding frequencies have been estimated to be

$< 3 \cdot 10^{-7}/a$ in the first case and $< 3 \cdot 10^{-8}/a$ in the second case (see section 5.1.1). If the leak is not detected, for the transition probability as an upper estimation a value of 1 is used. With a frequency of $< 3.0 \cdot 10^{-8}/a$ for a not detected flooding of the reactor building annulus, a frequency of $< 3.0 \cdot 10^{-8}/a$ for the occurrence of a core damage state is calculated. In comparison, the core damage frequency caused by flooding, which leads to a transient due to a failure of the personnel to isolate the leak (but not to detect the leak), is neglected. The probability for the transition from the initiating event (frequency $< 3 \cdot 10^{-7}/a$) to core damage is estimated to be significantly $< 1 \cdot 10^{-1}$, since secondary side systems are available for residual heat removal and manual actions are still possible.

- **Transients induced by a cable fire inside the containment**

As initiating events induced by a cable fire inside the reactor containment transients (loss of a main coolant pump, malfunctions of the feedwater supply to a steam generator) with a frequency of $1,8 \cdot 10^{-5}/a$ have been investigated. The frequency of additional failures (e.g. LOCA as consequence of opening of pressurizer valves, loss of more than one main coolant pump, malfunctions of the feedwater supply to more than one steam generator) as a consequence of the fire propagating to cable distributions of other redundant trains is estimated to be $< 1 \cdot 10^{-8}/a$ due to the results of the fire event sequence analysis.

For the selected fire scenario (see section 5.2.2) the fire effects (e.g. temperatures, pressure) including their time dependant development in the fire near field as well as in other areas inside the containment have been calculated. To consider methodical effects on the results, and to assure the quality of the results, two types of fire simulations have been performed. In a first step, the fire near field was modeled with a validated multi-compartment multi-zone model CFAST. In a second step, some selected calculations for the near as well as for the far field have been performed with the lumped parameter code COCOSYS developed by GRS. For these calculations, the same energy source terms have been assumed as for the CFAST simulations.

Probabilistic assessments have been carried out to estimate the frequency of cable fires in this plant area and to assess the reliability and efficiency of the fire extinguishing measures. Due to the favorable results of the fire modeling, rough and simple estimates have been satisfactory for assessing the consequences of such a fire on safety

systems and safety related equipment. In-depth systems analysis would have caused methodical problems.

Starting with a low occurrence frequency ($1,8 \cdot 10^{-5}/a$) of transients induced by a fully developed fire in the redundant train to be analyzed and due to the fact that the reliability of systems to cope with such transients is not significantly affected by the fire, the contribution of this event analyzed in detail to the system damage frequency is negligible. With respect to the frequency of the triggering event the results for the potential consequences in the area analyzed also cover the other three redundant areas. Therefore, the contributions from a fire in one of these other cable distributions are negligible. This is also valid for the core damage frequency, because it can be assumed that the possibility of plant internal accident management measures is not significantly affected.

The results of the fire simulations have demonstrated that the temperatures in the adjacent redundant trains do neither reach failure temperatures nor ignition temperatures of cables, even if there is no fire extinguishing. These results have been ensured by detailed uncertainty analysis. Thus, a fire propagation by thermal effects can be excluded. A cross-check of the plant specific conditions gave no indications for a fire propagation via cables connecting redundant trains. Even under consideration of the uncertainty of this diagnosis, the probability of fire propagation via this way is extremely low. The probability of a fully developed fire in one redundant train propagating to adjacent redundant trains with a consequential event sequence resulting in core damage state is estimated to be $< 10^{-3}$. Due to this, for this fire event sequence no relevant contribution to the system damage and core damage frequencies is to be assumed.

With respect to the contribution to the core damage frequency with an early release of radioactive material to the environment (plant damage frequency) in the frame of a level 2 PSA, the investigations have demonstrated that the triggering event fire itself does not affect the containment, even if the fire extinguishing is not successful. It therefore can be assumed that the possibilities for fires inside the containment do not lead to a relevant contribution to the plant damage frequency.

5.1.2.3 Transients caused by external area events

External area events (aircraft crash, explosion pressure waves, earthquake, flooding, extreme weather conditions including lightning) have not been analyzed in detail in this

PSA, either because their influence on the results for core damage states and for the level 2 of the PSA is low or because reliable methods for a detailed assessment are not available. Their potential contribution to the frequency of damage states is estimated in the following. These estimations start with triggering events. Table 5.3 gives an overview on the triggering events and their influence on the PSA.

Table 5.3 Relevant frequency intervals of the estimated triggering events

Triggering event	Frequency intervals [1/a]		
	A	B	C
Earthquake	< 1E-4	n. e.	n. e.
Aircraft crash	1E-5 up to 1E-9	> 3E-8	< 1E-8
Explosion pressure wave	5E-7 up to 5E-8	> 1E-8	< 1E-8
Extreme flooding	< 1E-2	> 1E-4	low or n. q.
Extreme weather conditions	< 1E-2	> 1E-3	low or n. q.
Extensive failure of components with high energy capacity	n. q.	n. q.	n. q.

A with safety significance for the plant
 B covered by design
 C of plant damage states

n. e. not estimated
 n. q. not quantifiable

- **Earthquake**

Seismic hazards have been assessed neither quantitatively nor qualitatively in this PSA. The reasons are the following:

- A probabilistic assessment of the seismicity at the site of the reference plant complying with the current state of the art was not available to GRS. A completely new assessment would have gone beyond the frame of this PSA.
- The methods for the evaluation of the earthquake induced failure probability of buildings and technical installations are altogether not yet developed so far, that reproducible and reliable results can be gained with an analytical effort, which is proportionate compared to the whole PSA.

- **Aircraft crash**

The design of the reference plant against aircraft crash meets the current German requirements, which apply the highest load assumptions by international comparison. In this way, a great deal of conceivable scenarios in case of a crash of military or civil aircraft are covered. Loads, which exceed the design limits and can lead to a core damage with simultaneous containment failure, can be practically excluded (frequency $< 10^{-8}/a$) /HAI 01/.

- **Explosion pressure waves**

The reference plant is also designed against explosion pressure waves according to currently valid requirements with – by international comparison - high load assumptions. Starting from a low accident frequency of transportation by ship - relevant in this respect - on the river Neckar, a frequency $< 10^{-8}/a$ is estimated for exceeding the design loads. A detailed analysis of these events does not seem to be necessary even for a level 2 PSA.

- **Extreme flooding**

A relevance of the event "extreme flooding" for a level 2 PSA is not seen, because of the favorable site conditions (asymptotically limited maximum water levels, possibilities for relief at barrages downstream of the river), of the design of the plant complying with current requirements and due to the fact, that the plant has to be shut down in case of extreme flooding and that all measures are aimed to ensure the residual heat removal. However, a reliable approach to quantitatively support this estimation is presently not available.

- **Extreme weather conditions**

A qualitative assessment of the potential consequences of extreme weather conditions shows that the safety relevant buildings of the reference plant – due to their design against aircraft crash and explosion pressure waves - can withstand much higher impacts from wind pressure or snow loads than to be considered for the typical central European climate. Nevertheless, the potential consequences in case of destruction of not specially protected operational installations, such as loss of auxiliary power supply

and loss of the cooling water supply, are considered in the PSA as accident initiating events. For the evaluation of initiating event frequencies also causes due to extreme weather conditions are considered. Therefore it can be assumed that these events are implicitly taken into account in the PSA.

Extreme weather conditions leading to beyond design loads not implicitly considered in the PSA cannot be completely excluded. However, their frequency cannot be derived even from long-term weather observations. Models for a theoretical evaluation of such a frequency are not yet available.

Also with respect to effects of lightning it can be principally assumed that they are implicitly considered in the data evaluation in the PSA. This is valid at least for the frequency of initiating events. High voltages induced in the electric power supply resp. in the instrumentation and control (I&C) system by lightning may lead to failures of components. These failure are taken into account in the data evaluation. Potential consequences of such strokes of lightning, whose effective parameters are not covered by the lightning protection plant design, are not considered. Although such strokes of lightning are rare, their consequences, particularly on the I&C system, have not been analyzed in much detail up to now according to our knowledge and they are presently not considered in the PSA.

With respect to providing cooling water for safety systems in cases of extreme dry weather periods, in our opinion the amount of river water which has be provided to the auxiliary service water supply in case of the plant being shut down can be always achieved. In future PSA, the possibilities of a loss of service water supply should be further analyzed (e.g. with regard to a failure of barrages with the corresponding changes of water levels).

5.1.2.4 Extensive failure of components with high energy capacity

Extensive failures of components with high energy capacity are not analyzed in detail in the present PSA. The reason is that either the effects on the frequency of core damages states and for a level 2 PSA are low or that a reliable method for a detailed assessment is not yet available. The potential contribution to the damage state frequencies is estimated in the following. These estimations are based on triggering events (see table 5.3).

For the definition of initiating events only limited damages (e.g. main coolant line leaks $< 0,1F$) at the pressure bearing barrier are assumed for passive components (vessels and pipes with high energy capacity). Other damages are not considered, since the break preclusion has been demonstrated for all components to come into question. The technical requirements to be fulfilled are defined in the nuclear standards. For 20 years, this procedure is part of the German licensing practice. The demonstration of break preclusion is mainly based on meeting technical requirements from experience, results from experiments performed in reactor safety research programs demonstrating the load bearing characteristics of components with differing deficiencies in quality, the continuous evaluation of the operating experience (national and international), analysis of crack growth of postulated defects, an early detection of defects by means of in-service inspections and plant monitoring, and by demonstrating sufficient load bearing possibilities of cracked components in case of accidental loads. Quantitative methods for estimating the failure probabilities of passive components under loads in case of anticipated operation as well as in case of accidents are limited with respect to their potential applications and to their theoretical basis. Furthermore, the required input information for such calculations is not available in the necessary type and from (parameter distributions for independent and dependent data).

With regard to the very low core damage frequencies resulting from the event sequences investigated for GKN 2, it has to be discussed if the break preclusion for components with high energy capacity can be anymore considered as sufficiently justified. In this context potential contributions to the core damage frequency and to the frequency of radioactive nuclide releases induced by an impairment of containment integrity in case of controlled or uncontrolled LOCAs have to be considered. All vessels and pipes with high energy capacity inside the containment have to be treated accordingly.

In these investigations for the GKN 2 plant independent analyses for a quantitative assessment of the reliability of passive components were not planned. For such analyses, the available models would need to be improved. In the following it is discussed to what extent the basic assumptions of the break preclusion concept (precautions against all conceivable damage mechanisms and timely detection of potential damages) can be assumed to be still valid, taking into account the grown operating experience and the advanced state of knowledge. This is done in the form of subjective expert judgment.

GKN 2 belongs to the latest level of development of pressurized water reactors for which requirements of basic safety have been applied for all components from the be-

ginning. This means, compared to earlier levels of development, that the components have been erected in optimized production quality, and, therefore, higher safety margins are available against operational loads and effects of potential damages. The following damage mechanisms affecting the component integrity have to be considered for pressurized water reactors:

- Changes in the material characteristics by neutron radiation with high energies
- Fatigue due to cyclic loading
- Crack initiating due to corrosion attack
- Wall thinning due to corrosion effects
- Unstable crack propagation in case of loads exceeding the material specific value
- Plastic instability in case of loads exceeding the material specific strength

In the following, the above mentioned aspects are discussed and it is shown, to what extent the safety margins of GKN 2 are to be estimated in comparison to the internationally available knowledge and in how far the state of knowledge concerning the development of the potential damage mechanisms is covered by the given plant operation periods.

- Changes in the material characteristics by neutron radiation with high energy
Due to the requirements in the German standards, changes in the material characteristics by high energy neutron radiation are low and limited to the area of the reactor pressure vessel close to the core. A broad data basis is available from the investigations performed with surveillance samples for all German pressurized water reactors. The existing data set will be further validated by additional investigations to be performed. A comparison of characteristic parameters, e.g. the displacement of the brittle fracture transition temperature due to neutron radiation, shows that the values for reactor pressure vessels of Konvoi-type PWR are more than a factor 2 lower than for many other PWR worldwide. The very limited change of the material characteristics close to the core is not significant for the reactor pressure vessel of GKN 2 NPP.
- Fatigue due to cyclic loading
Due to the extensive operating experience with pressurized water reactors, those component areas, for which a higher fatigue value can occur, can be reliably narrowed. As a consequence of the optimized construction and manufacturing conditions for vessels and piping with high energy capacity the number of areas with higher stress is lower in comparison to former PWR generations. The inspection concept and the specific fatigue monitoring consider the experience with for

PWRs. Damages which occurred up to now have been limited to piping with small diameters, for which breaks are assumed anyway in the safety verification. The respective sequences have been also investigated in the present study. For the components and piping considered in this framework, no cracks induced by operation have been observed up to now. Similar components of other PWRs from foreign manufacturers showing up single cracks due to fatigue indicate that a crack growth due to fatigue is not frequent for PWR specific service loading conditions. Plant operational periods of up to 30 years without any component failures are available for a variety of nuclear power plants with much lower safety margins than those of GKN 2 (higher notch stresses, more unfavorable material conditions). A deterioration by fatigue of the integrity of the components to be considered in this framework can be excluded due to the extensive experience available.

- Crack initiation due to corrosion attack

The available operating experience does not give any indication that the integrity of the pressure bearing wall of the components to be considered can be affected by corrosion mechanism with crack initiation and growth. Damages observed up to now affect only small piping or occur under conditions (water chemistry, materials), which cannot be applied to components of GKN 2. Furthermore, the worldwide operating experience, covering also damages with stress corrosion cracking, indicates that potential crack growth velocities are limited so that potentially occurring damages can be observed timely during the in-service inspection periods. In addition, long lead time periods are available for the feedback because of the variety of operating PWR with lower safety margins. By this means it is possible to implement preventive measures in time against unexpected damage sequences.

- Wall thinning due to corrosion effects

In the primary circuits of PWRs a local corrosion of pressure bearing walls can occur induced by locally limited leaks (e.g. at parts of seals), by evaporation of liquids and by a local increase of the boron concentration. This corrosion mechanism has caused significant damages worldwide, since in part also bolted joints important for the integrity of components have been extensively damaged. Due to the typical operation modes in Germany, which does not permit a long-term operation with reactor coolant leakages, similar damages did not occur in German PWRs. Because this operation mode is also practiced at GKN 2, and due to the

5 Level 1 PSA for power operation

available leak detection, damages induced by boron acid corrosion resulting in endangering the component integrity can be excluded.

- Plastic instability in case of loads exceeding the material specific strength (crack resistance)

The high ductility of all materials and welds of pressurized components, required by the German standards, ensures that high safety margins against unstable crack propagation are available. All materials are thermally stable for the occurring operational condition, so that the material characteristics are not affected. The effects of neutron radiation are limited (see also “changes in the material characteristics by neutron radiation with high energy“).

- Plastic instability in case of load exceeding the material specific strength
Because of the reliable equipment for pressure limitation, no sequences have been found in all investigations questioning the integrity of pressurized components in case of loads from anticipated operation and in case of accidents. Potentials for failures of components during beyond-design accidents need not to be considered in this context.

These qualitative considerations show that from the operational experience and from the results of reactor safety research programs there are no indications to call in question that the prerequisites of the break preclusion concept are met. The components to be considered have been operated without any damage up to now. Also from comparable plants there are no indications of incipient damages which could impair the integrity. The examination of the worldwide operational experience shows only a low number of limited damages for components with considerably lower safety margins and longer operational periods. In case of accumulation of damages (boron corrosion) corrective actions have been taken quickly. A loss of integrity of vessels and piping with high energy capacity inside the containment is not to be treated as triggering event. If unexpected new damage mechanisms would be detected for plants with much lower safety margins compared to GKN 2, the lead time would be large enough for taking appropriate corrective measures for the prevention or limitation of damages.

5.1.2.5 Synopsis on neglected contributions to core damage and release frequencies

Table 5.4 summarizes the estimated contributions to core damage and release frequencies induced by initiating events, which have not been further analyzed (see sections 5.1.2.1 to 5.1.2.4). Frequencies and characteristics of the release categories FKA - FKJ evaluated in level 2 of the PSA can be found in table 6.11. The contributions to the frequencies of the categories with the highest releases, FKA and FKB, are listed separately, the contributions to the frequencies of other categories (FKC - FKJ) have been combined. The frequency contributions to the release categories have been estimated based on the results of the level 2 of the PSA for the contributions of the analyzed initiating events to the release categories (see table 6.11). For example, for the large and medium leak at a main coolant line the contributions found for leaks $> 25 \text{ cm}^2$ have been applied (column L > 25 in table 6.11). For interfacing system LOCAs and for ATWS additional estimations for the contributions of the release categories are available.

The contribution of initiating events, which have not been further analyzed, to the frequency of the release category FKB, listed in table 5.4, represents approx. half of the frequency of this release estimated within the level 2 of the PSA. In this context, it has to be taken into account that the frequency of $< 7 \cdot 10^{-9}$ represents a pessimistic upper limit. Furthermore, this value is very low compared to the frequency of the release category FKA ($2.1 \cdot 10^{-7}$) with is connected with significantly higher consequences than FKB.

5.2 Transition from initiating events to system damage states

Per design, initiating events are controlled by the available system functions. Only those event sequences can lead to system damages states, for which the system functions required for core cooling fail. The event tree analysis investigates – starting with the initiating event - the event sequences and resulting plant states, which can occur depending on the availability of the system functions required to cope with the initiating events. Plant states, for which the core cooling has failed in such a way that a core damage can be prevented only by plant internal accident management or repair measures, are designated as system damages states. Depending on the initiating event and the event sequence, system damages states with different characteristics can occur. In

5 Level 1 PSA for power operation

the PSA 12 different system damage states are distinguished. They are summarized in the first column of table 5.5 and characterized as follows:

- Loss of secondary-side (S) resp. primary-side (P) system functions for heat removal
- Pressure in the primary circuit (LP = low, MP = medium, HP = high)
- Time window available for the prevention of core damage states. The specified time periods are based on estimations /PÜT 01/.

Table 5.4 Estimated frequencies of core damage states and release categories for those events which have not been analyzed in detail

No. ¹⁾	Initiating event	Frequency [1/a]			
		CDS	FKA	FKB	FKC-FKJ
1	Large and medium leak at a main coolant line	< 1E-9			< 1E-9
5	Small leak at the pressurizer induced by transients	1E-9	<< 1E-9		1E-9
7	Interfacing systems loss-of-coolant accident	< 1E-8	< 1E-9	< 7E-9	< 3E-9
9	Steam generator tube leak 6 - 12 cm ²	4E-9	3E-9		1E-9
14	Steam generator overfeeding	1E-8	1E-9		9E-9
16	Main steam line break inside the containment	< 1E-9	<< E-9		< 1E-9
18	Feed water line break inside the containment	< 1E-9	<< E-9		< 1E-9
19 to 22	ATWS	< 1E-9			< 1E-9
23	Transient caused by fire extinguishing system leak inside annulus ³⁾	< 3E-8	< 3E-9		< 3E-8
24	Transient caused by fire inside the containment	< 1E-8	1E-9		9E-9
2)	Extensive failure of components with high energy capacity	n.q.			
2)	External hazards	< 2E-8	< 2E-8		
Sum of the neglected contributions:		< 9E-8	< 3E-8	< 7E-9	< 6E-8
Total values estimated for level 1 and level 2 (see tables 5.20 and 6.11)		2.5E-6	2.1E-7	1.3E-8	2.3E-6

1) see table 5.1

2) see table 5.3

3) reactor building annulus

ATWS anticipated transients without scram

FKA-FKJ release categories, see table 6.11

CDS core damage states

n.q. not quantified

For the event tree analysis it has first to be assessed, which system functions are required to cope with an initiating event. For this assessment, generally the system requirements verified and determined in the nuclear licensing process have been used. For system functions, which are relevant for the results, thermal hydraulic analyses have been performed for the PSA /GRS 98/, /HOL 99/, /PÜT 01/.

Applying the methods of the event tree and fault tree analysis in the PSA the probabilities have been evaluated, that an initiating event is not controlled by the system functions as designed and, therefore, the event sequence leads to a system damage state.

The system functions required to cope with the individual initiating events are discussed in the following sections 5.2.1 to 5.2.11. In these sections also the results of the numerical calculations of the event and fault tree analyses are outlined, in detail:

- the probabilities for transition from the initiating event to system damage states,
- characteristic parameters of the system damage states relevant for the results,
- contributions from failures of individual system functions, and
- contributions of individual failure causes, of common cause failures (CCF) and human failures.

If not explicitly mentioned, the presented results are mean values calculated by the uncertainty analyses.

The results have been calculated by evaluating the minimal cuts taking into account the uncertainties of the reliability data. For this purpose, Monte Carlo simulations with a sample size of 5.000 each have been performed. The estimated mean values of the system damage frequencies are higher than the point values (calculated from the mean values of the reliability data) (see section 5.4).

- **Evaluation of the transition probabilities**

The transition probabilities are equivalent to unavailabilities – averaged over the observation period (one year) - of those system functions, whose failures lead to the corresponding system damage state. Average unavailabilities are calculated, because the unavailabilities of the system functions can differ over the time period, and the point of time of the system function demand is random (point of time of occurrence of an initiating event). The unavailabilities of the same system function at different points of time of

demand are different, if the reliability of the component functions which are relevant for the system functions is described by failure rates. This is the preponderant case in this PSA. The average unavailabilities are calculated by numerical integration of the time-dependent unavailabilities over the observation period and the following division by the length of the observation periods (in the following average unavailabilities are briefly designated as unavailabilities).

The transition probabilities from the initiating event to a system damage state are calculated on the basis of the evaluations of the different uncontrolled event sequences (paths) in the event trees. The failure combinations, leading to the respective system damage state, are calculated for each of these paths, numerically evaluated and subjected to an uncertainty analysis. With respect to different system damages states further branches had to be added and numerically evaluated in individual cases. On the other hand, several paths were assigned to the same system damage state, if the characteristic parameters were the same. For these cases the mean values for the transition probabilities were summed up. Accordingly, the frequencies of the individual system damages states add up to the total frequency of the event "system damage state" for an initiating event. The available PSA computer codes do not take into account the probabilities of "non-failures" (i.e. for intact states). In principle, this approach is overestimating of the total values for the transition probabilities. For a more detailed explanation, the following example of a small leak at the main coolant line, 2 - 25 cm² (see section 5.2.3) is used:

For the event sequences it is differentiated whether the main steam collector is available or has failed (e.g. because the main steam bypass system opens too fast and therefore the isolation signals for the collector are actuated). Furthermore it is distinguished whether the low pressure injections are available or not. A loss of the low pressure injections leads to a system damage state. For both cases (with or without main steam collector) the low pressure injections can fail because of a CCF of all four residual heat removal (RHR) pumps, which would induce a system damage state. Therefore, this CCF is one of the minimal cuts for a small LOCA, which are found from an evaluation of the uncontrolled path with "main steam collector available" AND "low pressure injections failed". From the evaluation of the likewise uncontrolled path with "main steam collector failed" AND "low pressure injections failed", one of the failure combinations is "main steam bypass system opens too fast" AND "CCF of all four RHR pumps". This failure combination is not a minimal cut and therefore is not to be added

to the total frequency of a system damage state for a small leak at a main coolant line, 2 - 25 cm².

The influence of this simplification is less than 3 % of the transition probability per initiating event.

- **Evaluation of the frequencies of system damage states**

For the evaluation of the frequencies of the individual system damages states the uncertainties of the initiating event frequencies have been taken into account. For a Monte Carlo simulation with a sample size of 5.000 each frequency has been multiplied by the respective value of the transition probability. The frequencies of the individual system damages states are calculated by summing up the products and dividing the sum by 5.000. The result may be different from the results which would be gained by multiplication of the individual estimated mean values of the frequencies of the initiating events and the transition probabilities. The deviations decrease with increasing sample size and they are insignificant already with a sample size of 5.000.

- **Evaluation of the contributions from individual system functions**

The mean values for the contributions of individual system functions to the system damage frequency have been evaluated from the uncertainty analysis.

- **Evaluation of the contributions from individual failure causes (importances)**

In order to evaluate the contributions of individual failure causes and the contributions of common cause failures (CCF) and human failures to the system damage frequency from an initiating event, the failure combinations (all uncontrolled paths together) have been calculated separately and evaluated with respect to the failure causes.

- **Tabular presentation of results**

The results for system damages states are summarized in tables 5.5 and 5.6.

Table 5.5 shows the probabilities for the transition from initiating events to system damage states. In the table also the mean values of the frequencies of the system damage states are given.

In Table 5.6 the mean values of the unavailabilities of the required system functions, the main contributions to the mean values of the unavailabilities, and the contributions from CCFs and from human failures (HF) are compiled for the plant internal initiating events. Furthermore, the mean values of the frequencies of the system damages states (primary-side, secondary-side and combinations from primary-side and secondary-side failures) as well as their sums are given.

5.2.1 Small leak at a main coolant line, 80 - 200 cm²

- **System functions required to cope with the initiating event**

The reactor is made subcritical by reactor scram. During cooldown of the plant subcriticality is maintained by injection of borated water by the emergency core cooling system resp. the volume control system. The following system functions are required for core cooling:

In case of a leak of 80 to 200 cm² a high pressure injection by at least one train is required, whereby it is assumed that an injection into the leaking circuit is not efficient.

Table 5.5 Probabilities of the transition from initiating events to system damage states

No	System damage states				Transition probabilities of the			
	Designation		f [1/a]	2	MCLL		PL	6
	FC	P			t [h]	3	4	
				9.0E-5	1.5E-4	3.0E-3	8.5E-4	
1	<u>PS</u>	MP	< 1	2.4E-7	5.8E-4	2.0E-4		2.0E-4
2	<u>PS</u>	MP	1 - 1,5	2.2E-8			6.7E-6	
3	<u>PS</u>	MP	2 - 3	6.3E-8		4.8E-4		
4	<u>PS</u>	LP	2 - 4	2.8E-7	3.6E-4	2.9E-4		2.8E-4
5	<u>PS</u>	LP	> 4	8.7E-7			3.0E-4	
6	<u>PS</u>	HP	1 - 2	4.6E-7			9.1E-5	
7	<u>PS</u>	HP	2 - 3	5.9E-6				
8	<u>PS</u>	MP	> 10	1.6E-7				
9	<u>PS</u>	MP	> 12	6.5E-8		1.0E-4	1.4E-5	
10	<u>PS</u>	MP	2	5.8E-9		3.3E-5		2.1E-6
11	<u>PS</u>	MP	2 - 3	2.6E-8				
12	<u>PS</u>	MP	> 4	9.0E-8			3.0E-5	

- | | | | |
|----------|---|------|----------------------------|
| 1) | see table 5.1 | HP | high pressure |
| FC | failure cause | MP | medium pressure |
| P | pressure in | LP | low pressure |
| MS | main steam | SGTL | steam generator tube leaks |
| FW | feedwater | PL | pressurizer leak |
| f | frequency | MCLL | main coolant line leaks |
| t | time window for accident management measures and repair | | |
| <u>P</u> | failure of primary-side system function | | |
| <u>S</u> | failure of secondary-side system function | | |

initiating events ¹⁾ (Event group, number, frequency [1/a])							
SGTL	Anticipated transients					MS FW leaks	
8	10	11	12	13	15	16	
2.3E-3	2.5E-2	1.2E-1	3.8E-2	7.5E-3	1.6E-4	2.6E-4	
	2.5E-6	9.6E-8	2.5E-6	2.5E-6	2.5E-6	2.5E-6	
	5.2E-5	1.9E-5	4.0E-5	3.7E-5	8.1E-4	1.1E-3	
7.2E-5							
1.4E-5							



If at least two high pressure trains inject into intact loops a secondary-side heat removal is not required. Otherwise the plant has to be cooled down via the secondary circuit.

For secondary-side heat removal steam generator feeding by one main feedwater pump or by two start-up and shutdown pumps is sufficient. If these operational systems fail, at least two steam generators have to be fed by the emergency feedwater system. The plant must be cooled down with a temperature gradient of approx. 100K/h, whereby the main steam can be released via the main steam bypass system or at least one of the four main steam relief control valves.

Table 5.6 Unavailabilities of system functions and the frequencies of system damage

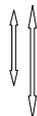
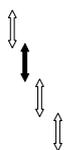
No.	Initiating event Designation	1) f [1/a]	UA	Unavailabilities of
				Main contributions System functions
2	Small leak at MCL, 80-200 cm ²	9.0E-5	9.4E-4	HP injection LP injection
3	Small leak at MCL, 25-80 cm ²	1.5E-4	1.1E-3	HP injection LP injection FW supply
4	Small leak at MCL, 2-25 cm ²	3.0E-3	4.4E-4	LP injection FW supply 100K/h-cooldown and HP/LP-injection from Sump
6	Small leak at pressurizer, 40 cm ²	8.5E-4	4.8E-4	LP injection HP injection
8	SG tube leak, 1-6 cm ²	2.3E-3	8.6E-5	Isolation and long-term heat removal Prevention of emer- gency core cooling criteria and HP injection
10	Loss of preferred power	2.5E-2	5.5E-5	FW supply MS pressure control/limitation
11	Loss of MFW without loss of MHS	1.2E-1	1.9E-5	FW supply
12	Loss of MHS without loss of MFW	3.8E-2	4.3E-5	FW supply MS pressure limitation
13	Loss of MFW and loss of MHS	7.5E-3	3.9E-5	FW supply MS pressure limitation
15	MS line break outside the containment	1.6E-4	8.1E-4	Separation of the MS system
16	FW line break outside the containment	2.6E-4	1.1E-3	FW supply

1)	see table 5.1	f	frequency	HF	human failure
SG	steam generator	HP	High pressure	LP	low pressure
MCL	main coolant line	UA	unavailability		
MS	main steam	MFW	main feedwater		
CCF	common cause failures	MHS	main heat sink		
		FW	feedwater		

5.2 Transition from initiating events to system damage states

states of initiating events

system functions %	Amount [%]		System damages state frequencies [1/a]			
	CCF	HF	Failure cause			Total value
			PS	PS	PS	
62 38	37	2	9.0E-8			9.0E-8
62 26 8	46	1	1.4E-7	1.6E-8	4.6E-9	1.6E-7
68 21 7	73	4	8.7E-7	3.3E-7	1.1E-7	1.3E-6
58 42	59	1	4.0E-7		1.8E-9	4.0E-7
83 17	88	40	1.9E-8	1.6E-7	7.0E-9	1.8E-7
95 5	95	0		1.4E-6		1.4E-6
99	97	0		2.2E-6		2.2E-6
94 6	94	0		1.8E-6		1.8E-6
94 6	93	0		3.0E-7		3.0E-7
86	89	0		1.3E-7		1.3E-7
99	68	0		2.9E-7		2.9E-7
Total			1.5E-6	6.6E-6	1.2E-7	8.2E-6



With the high pressure injections resp. the secondary-side cooldown together with the energy discharge via the leak the pressure in the reactor coolant circuit is decreased so

far that an injection by the residual heat removal (RHR) pumps is possible (low pressure injection). After the borated water storage tanks have been emptied to a minimum amount, the RHR pumps in recirculation mode begin to suck water from the containment building sump. For a cavitation free operation the RHR pumps the water level in the containment has to be sufficiently high. This requires the injection from at least two borated water storage tanks (via the high or low pressure injection system) or from one borated water storage tank and at least three accumulators (accumulator injection) in any circuit.

After the borated water storage tanks have been emptied by the high or low pressure injection system, the low pressure injection in recirculation mode is required. In this case, the injections have to be performed

- by a low pressure train via the hot and cold leg OR
- by at least two low pressure trains, each via at least one leg (hot or cold).

According to the minimum requirements for the injection the residual heat has to be removed via the corresponding RHR heat exchanger and the RHR chain.

In summary, the following system functions are distinguished for core cooling:

- High pressure injections by the safety injection pumps into at least one intact circuit (1 out of 3 HP injections)
- High pressure injections by the safety injection pumps into at least two intact circuits (2 out of 3 HP injections) OR
steam generator feeding and main steam release for plant cooldown with a gradient of 100K/h
- High pressure, accumulator, and low pressure injections for providing a sump water level being sufficiently high for a cavitation free operation of the low pressure pumps
- Low pressure injections in sump recirculation mode by the RHR pumps and residual heat removal via the RHR chain (2 out of 8 LP injections in sump recirculation mode).

- **Transition from the initiating event to system damage states**

For the transition from the initiating event "small leak at a main coolant line, 80 - 200 cm²" to a system damage state a probability of $9.4 \cdot 10^{-4}$ has been calculated. With an initiating event frequency of $9.0 \cdot 10^{-5}/a$ (see section 5.1.1) the frequency for the occurrence of a system damage state induced by a small leak at a main coolant line, 80 - 200 cm² is of $9 \cdot 10^{-8}/a$.

- **Characteristics of the system damage states**

The result is dominated by system damages states with a loss of primary side system functions, low resp. medium pressure in the primary circuit and a time window for the prevention of core damage states below 4 h (see table 5.5, system damages states 1 and 4).

- **Contributions of system function failures**

The unavailabilities of the high pressure injection (62 %) and of the low pressure injection (38 %) are the main contributors to the transition probabilities.

The loss of the three high pressure injections into the intact circuits is caused to approx. 50 % by failure combinations with a failure to run of the high pressure pumps. A major role with more than 40 % play also independent failures of the check valves in the hot and cold legs (primary isolation valves), which are tested only annually.

For the failure of the low pressure injections independent failures and CCFs of the level measurements in the cell cooler of the RHR chain play an essential role. These measurements, which are required for the function of the residual heat removal, with respect to the design (one channel) and to the interval of in-service inspections (yearly), do not conform to measurements in the reactor protection system. Furthermore, also for low pressure injections failures of the primary isolation valves are important.

- **Contributions of individual failure causes (importances)**

In summary, failures to open the primary isolation valves, failures of the high pressure pumps to run and independent failures of the level measurements in the cell coolers

bring the highest contributions to the transition probabilities from the occurrence of the small leak at a main coolant line, 80 – 200 cm², to a system damage state.

With a total contribution of approx. 37 %, CCFs are in comparison to other initiating events, e.g. anticipated transients with more than 90 %, by far less significant (see table 5.6). On the contrary, independent failures play a major role, whereby failure combinations with the same type of component failures give an essential contribution. The following four failure combinations alone contribute in total 30 % to the frequency of a system damage state with the independent failures of

- three primary isolation valves in the hot legs of the injection lines of the emergency core cooling system,
- three primary isolation valves in the cold legs of the injection lines,
- three high pressure pumps (failure to run), and
- four level measurements in the cell coolers of RHR chain.

These results are affected by the fact, that the importances of the component failures have been calculated under consideration of reliability data distributions and their dependencies (“failure rate coupling“, see section 5.4). If “point value calculations“ are used, the importances may be wrongly assessed. In this case the four above mentioned failure combinations would contribute only about 2 % to the result.

Human failures play a minor role with a contribution of less than 2 % in case of a small leak at the main coolant line, 80 - 200 cm² (see table 5.6). The contributions come from failures of manual actions in connection with a loss of the water supply to the cell coolers in the RHR chain.

5.2.2 Small leak at a main coolant line, 25 - 80 cm²

- **System functions required to cope with the initiating event**

For defining the minimum requirements, thermal hydraulic calculations have been performed /HOL 99/. In comparison to a small leak at a main coolant line, 80 - 200 cm² (see section 5.2.1), the following differences have been found for the system functions required to cope with the initiating event:

Independent of the number of available high pressure injections, a secondary-side cooldown of the plant is required in order to reduce in due time the pressure in the primary circuit to a value which allows the injection by the low pressure pumps. If the main steam release via the main steam bypass system and all four main steam relief control valves fails, the small leak at a main coolant line (up to 80 cm²) can be controlled, if the "recirculation mode operation of the high pressure safety injection pumps" (with the low pressure pumps as pre-pumps) is actuated manually as planned in the protection goal oriented operating manual. For this purpose after a small leak at a main coolant line one of the three injections into the intact circuits is sufficient. In case of this operational state the plant has to be cooled down manually via a main steam safety valve within approx. 10 hours. Also this measure is planned in the protection goal oriented operating manual.

Another difference in the system functions required to cope with the initiating events concerns the low pressure injections. In case of sump recirculation mode an injection via at least one of the four hot injection legs or via one of the three cold injection legs of the intact circuits is required.

In summary, in case of a small leak at a main coolant line with a leak cross section of 25 - 80 cm² the following system functions are required for core cooling:

- High pressure injections by the safety injection pumps into at least one intact circuit (1 out of 3 HP injections)
- Steam generator feeding and main steam release for plant cooldown with a cooldown gradient of 100K/h OR
 - Suction by the high pressure safety injection pumps from the sump AND
 - cooldown with the main steam safety valves
- High pressure injections, accumulator injections and low pressure injections for achieving a sump water level being sufficient a cavitation free operation of the low pressure pumps
- Low pressure injections in sump recirculation mode via the RHR pumps and residual heat removal via the RHR chain (1 out of 7 LP injections in sump recirculation mode)

- **Transition from the initiating event to system damage states**

The probability for the transition from the initiating event "small leak at a main coolant line, 25 - 80 cm²" to a system damage state is approx. $1.1 \cdot 10^{-3}$. With the frequency of the initiating event of $1.5 \cdot 10^{-4}/a$ (see section 5.1.1) this leads to a frequency of $1,6 \cdot 10^{-7}/a$ for a system damage state induced by the small leak at a main coolant line, 25 - 80 cm².

- **Characteristics of the system damage states**

System damages states with loss of primary-side system functions contribute approx. 90 % to the result. In most cases the pressure in the primary circuit is between 1 and 10 MPa. The time windows available for the prevention of core damages states are between 1 and 4 h (see table 5.5, system damages states 1, 3, 4 and 10). In approx. 10 % of the system damages states the secondary-side cooldown has failed. In these cases, the available time windows are extended because the "high pressure injection in sump recirculation mode" is working (system damage state 9).

- **Contributions of system function failures**

Similar to the leak with a cross section of 80 - 200 cm², mainly failures of the high pressure injection (62 %) and of the low pressure injection (26 %) contribute to the transition probability of $1.1 \cdot 10^{-3}$. The remaining 12 % are caused by failure combinations with a loss of the feedwater supply (steam generator feeding) and failure of the automatic 100K/h-cooldown.

The causes for the loss of the high pressure injection are the same as for the small leak, 80 - 200 cm² (see section 5.2.1). The same is true also for the low pressure injections with the restriction that due to lower minimum requirements failures of primary isolation valves are less important. In return, CCFs of pumps and of valves in the RHR chain are of higher importance.

Failures of the feedwater supply for the steam generators mainly result from CCFs of valves (injection lines of the feedwater and emergency feedwater systems) and from failures to run of the emergency feedwater pumps resp. diesels and the demineralized water pumps.

A failure of the automatic 100K/h-cooldown results in a system damage state only if additionally

- the "high pressure injections in recirculation mode" either are not actuated timely or fail within approx. 10 h or
- the cooldown via the main steam safety valves is not successful (within 10 h).

In both cases, failures of the required manual actions play an essential role: approx. 30 % for the failure of the "high pressure injection in recirculation mode" and 100 % for unsuccessful cooldown via the main steam safety valves. For the failure of the high pressure injection in recirculation mode, besides the manual actions also the failure to run of the high pressure pumps, particularly in case of taking suction from the containment sump, plays an essential role (nearly 40 %). These pumps are not subject to periodic in-service inspections representative for the requirements in case of sump recirculation (with the low pressure pumps as pre-pumps).

The failure of the automatic 100K/h-cooldown results mainly from failures of the main steam release. Dominating are failure combinations with CCF of the relief control valves. These valves are required if the main steam bypass system is not available, whereby besides a loss of the main steam bypass system itself (failure to open) in particular failures of the operational steam generator feedwater supply are important, which lead to a blocking of the main steam bypass system by the condenser protection.

- **Contributions of individual failure causes (importances)**

Mainly independent failures of the primary isolation valves of the emergency core cooling system, failures to run of the high pressure pumps and independent failures of the level measurements of the cell coolers contribute to the transition probabilities from the small leak at a main coolant line, 25 - 80 cm², to a system damage state.

Failure combinations with CCF contribute in total approx. 46 %, human failures with less than 1 % play a subordinate role (see table 5.6). For both failure causes the statements in section 5.2.1 are valid.

5.2.3 Small leak at a main coolant line, 2 - 25 cm²

- **System functions required to cope with the initiating event**

For defining the minimum requirements, thermal hydraulic calculations have been performed /HOL 99/. The minimum requirements for the system functions are different from those for the small leak at a main coolant line, 25 - 80 cm², only in one point: for a small leak at a main coolant line, 2 – 25 cm², a high pressure injection by the safety injection pumps is not required, if the plant, as planned in the operating manual, is cooled down after occurrence of the leak with 100 K/h, if the main steam collector is available and if all four steam generators are supplied with feedwater. If the feedwater supply to one of the steam generator fails or if the main steam collector is isolated (by reactor protection signals after a too fast cooldown), the leak discharge rate increases. In this case, either a high pressure injection by the safety injection pumps into one of the three intact circuits or an injection from the accumulators into four circuits and by the extra borating system into the three intact circuits is required.

The system functions required for core cooling in case of a small leak at a main coolant line, 2 - 25 cm², are summarized as follows:

- main steam collector available
- if the main steam collector is available:
 - feedwater supply for four steam generators (4 out of 4) OR
 - one high pressure injection into an intact circuit (1 out of 3) OR
 - four accumulator injections (4 out of 4) AND three injections by the extra borating system into intact circuits (3 out of 3)
- if the main steam collector failed:
 - one high pressure injection into an intact circuit (1 out of 3) OR
 - four accumulator injections (4 out of 4) AND three injections into intact circuits by the extra borating system (3 out of 3)
- steam generator feedwater supply and main steam release for cooldown of the plant with a cooldown gradient of 100K/h OR
 - suction of the high pressure safety injection pumps from the sump AND
 - cooldown via the main steam safety valves

- high pressure, accumulator, and low pressure injections for achieving a sump water level sufficient for a cavitation free operation of the low pressure pumps
 - low pressure injections in sump circulation mode with the RHR pumps and residual heat removal via the RHR chain (1 out of 7 LP injections in sump recirculation mode)
- **Transition from the initiating event to system damage states**

The probability for the transition from the small leak at a main coolant line, 2 - 25 cm², to a system damage state is $4.4 \cdot 10^{-4}$. With the frequency of the initiating event of $3.0 \cdot 10^{-3}/a$ (see section 5.1.1) this leads to a frequency of $1.3 \cdot 10^{-6}/a$ for a system damage state induced by a small leak at a main coolant line, 2 - 25 cm².

- **Characteristics of the system damage states**

System damages states characterized by the loss of primary side system functions, low pressure in the primary circuit (< 1 MPa) and a time window of more than 4 h (see table 5.5, system damage state 5) contribute approx. 68 % to the result.

The remaining 32 % come mainly from secondary-side system function failures (24 %) resp. from primary- and secondary-side system function failures (7 %) (system damage states 6 and 9 resp. 12).

The system damage states 6 and 9 differ from each other by the pressure in the primary circuit and by the time windows. For system damage state 6 the pressure is high (response pressure of the pressurizer relief valve, approx. 17 MPa) and the time window is 1 to 2 h. However, this state is reached only for a part of the small leaks at a main coolant line, 2 - 25 cm², namely for smaller leak cross sections (2 - 12 cm²). The other cases are characterized by much lower pressures in the primary circuit (1 to 10 MPa) and extended time windows (by the function of the high pressure sump recirculation more than 12 h). Considering the frequencies (see section 5.1.1) for small leaks, 2 to 12 cm² resp. > 12 cm², system damage state 6 contributes about 20 % to the frequency of system damage states from a small leak at a main coolant line, 2 - 25 cm². The system damage states 9 (medium pressure, time window more than 12 h) and 12 (medium pressure, time window more than 4 h) together contribute approx. 10 % to the

frequency of system damage states from a small leak at a main coolant line, 2 - 25 cm².

- **Contributions of system function failures**

With 68 % of the frequency of the system damage states failures of the low pressure injections in sump recirculation mode deliver the highest contribution. Different from the leaks at a main coolant line with leak cross sections > 25 cm², the failure of the high pressure injections does not play a noteworthy role (< 2%), because an injection at a primary circuit pressure of more than 1 MPa (i.e. low pressure injections are not yet efficient) for a leak considered here (2 - 25 cm²) is required only after a loss of the main steam collectors resp. a failure of the feedwater supply to individual steam generators. The loss of the steam generator feedwater supply contributes 21 %, the remaining approx. 10 % result mainly from failures of the automatic 100K/h-cooldown with additional loss of the high pressure injection in sump recirculation mode.

The loss of the low pressure injection, as in case of a small leak at a main coolant line, 25 - 80 cm², is caused mainly by independent failures and by a CCF of the water level measurements in the cell coolers of the RHR chains, and CCFs of pumps and valves of the RHR chain.

The loss of feedwater supply of the steam generator is caused mainly by CCFs of valves (feed lines of the main feedwater and of the emergency feedwater system) and by failures to run of the emergency feedwater pumps resp. diesels and the demineralized water pumps.

The loss of the automatic 100K/h-cooldown is induced mainly (approx. 98 %) by failure combinations with CCF of the main steam relief control valves. The main steam relief control valves are required, if the main steam bypass system is not available. Besides the loss of the bypass system (failure to open) and the isolation of the main steam collector (bypass system opens too fast), mainly the blockage of the bypass system by the condenser protection due to a too high water level in the feedwater tank contribute to this situation. The water level increase in the feedwater tank is caused by failures in the operational feedwater supply.

The loss of the automatic 100K/h-cooldown alone does not lead to a system damage state. A system damage state only occurs, if additionally the high pressure injection in

sump recirculation mode additionally fails (actuation too late or failure to run within 10 h) or if the manual cooldown via the main steam safety valves fails. In both cases, failures of the required manual actions play an important role: approx. 30 % for the failure of the high pressure injection in sump recirculation mode and 100 % for the failure to cooldown the plant via the main steam safety valves. If the high pressure injection in sump recirculation mode fails, not only the manual actions but also the failure to run of the high pressure pumps, particularly in sump recirculation mode, are important (nearly 40%). These pumps are not subject to regular in-service inspections representative for the requirements in case of sump recirculation mode (with the low pressure pumps as pre-pumps).

- **Contributions of individual failure causes (importances)**

To the transition probability from a small leak at a main coolant line, 2 - 25 cm², to a system damage state the main contributions come from independent failures and CCFs of the water level measurements in the cell coolers of the RHR chain and from CCFs of valves in the main feedwater and the emergency feedwater system.

Failure combinations with CCF contribute in total with approx. 73 %, human failures with approx. 4 % are of minor importance (see table 5.6). For both failure causes the statements in section 5.2.1 are valid.

5.2.4 Small leak at the pressurizer by stuck open safety valve

- **System functions required to cope with the initiating event**

For the definition the minimum requirements thermal hydraulic calculations have been performed /HOL 99/. Different from the small leak at a main coolant line, in case of a small leak at the pressurizer by stuck open safety valve the high pressure resp. low pressure injections into all four primary circuit loops are effective. A further difference is, that a secondary-side heat removal is not required, if at least two high pressure injections work. Specifically, the following system functions are required to prevent system damage states,:

- high pressure injection by the safety injection pumps into at least one circuit (1 out of 4 HP injections)

5 Level 1 PSA for power operation

- high pressure injection by safety injection pumps into at least two circuits (2 out of 4 HP injections) OR
 - steam generator feedwater supply and main steam release for plant cooldown with a gradient of 100K/h OR
 - high pressure safety injection in sump recirculation mode AND cooldown with the main steam safety valves
- high pressure, accumulator and low pressure injections to achieve a sump water level sufficient for a cavitation free operation of the low pressure pumps
- low pressure injections in sump recirculation mode by the RHR pumps and residual heat removal via the RHR chain (1 of 8 LP injections sump recirculation mode)

- **Transition from the initiating event to system damage states**

The transition probability from a small leak at the pressurizer by stuck open safety valve to a system damage state is $4.8 \cdot 10^{-4}$. With the frequency of the initiating event of $8.5 \cdot 10^{-4}/a$ (see section 5.1.1) this leads to a frequency of $4.0 \cdot 10^{-7}/a$ for a system damage state induced by a small leak at the pressurizer by stuck open safety valve.

- **Characteristics of the system damage states**

The result is dominated by system damage states with failures of primary-side system functions, whereby 58 % are characterized by low pressure in the primary circuit and time windows of 2 to 4 h and 42 % by medium pressure in the primary circuit and a time window of approx. 1 h (see table 5.5, system damage states 1 and 4).

- **Contributions of system function failures**

The main contributions to the frequency of system damage states come from failures of the low pressure injections in sump recirculation mode (58 %) and of the high pressure injections (42 %). The failure of the automatic 100K/h-cooldown is not important for the frequency of system damage states from a small leak at the pressurizer by stuck open safety valve.

As with the small leak at a main coolant line, the main causes for a failure of the low pressure injection are independent failures and CCF of the water level measurements in the cell coolers of the RHR chain, CCFs of pumps and valves of the RHR chain.

Failure combinations with a failure to run of the safety injection pumps contribute 35 % to the failure of all four high pressure injections. Independent failures and CCFs of the primary isolation valves in the RHR system and CCFs of the safety injection pumps (failure to start) are also important.

- **Contributions of individual failure causes (importances)**

The highest contributions to the frequency of system damage states from a small leak at the pressurizer by stuck open safety valve come from independent failures of the water level measurements in the cell coolers of the RHR chain, from independent failures of the primary isolations in the RHR system, and from failures to run of the safety injection pumps.

Failure combinations with CCF in total have a contribution of approx. 59 %, human failures are of minor importance with 1 % (see table 5.6). For both failure causes the statements in section 5.2.1 are valid.

5.2.5 Steam generator tube leak, 1 - 6 cm²

- **System functions required to cope with the initiating event**

In case of a steam generator tube leak, 1 - 6 cm², system functions for the primary-side leak compensation, for the isolation of the damaged steam generator, and for the secondary-side heat removal are required.

With respect to the primary-side leak compensation it is distinguished whether a decrease of the pressurizer water level to < 2.28 m can be prevented or not. Because the pressure in the reactor coolant circuit drops to < 11 MPa due to the leak and the automatic coolant pressure reduction, the emergency core cooling criteria would be met at a water level of less than 2.28 m and the signals for the isolation of the primary circuit and of the containment would be actuated. The minimum requirements for the system function required to prevent the emergency core cooling criteria can be summarized as follows

- pressure reduction in the primary circuit by pressurizer spraying with two of the three high pressure charging pumps of the volume control systems or with one

high pressure charging pump and two extra borating pumps each in one of the two spray lines,

- leak compensation by injection into the primary circuit with two of three high pressure charging pumps or with one high pressure charging pump and two of the four extra borating pumps, whereby in both cases the high pressure reducing station must close to the minimum flow rate, and
- controlled main steam release, i.e. no primary-side sub-cooling by failures in the control of the main steam bypass system (opens too fast) resp. by a loss of the main steam bypass system due to failures in the release valve control.

- **Sequences with a failure of the system functions for the prevention of the emergency core cooling criteria**

If the emergency core cooling criteria cannot be avoided (loss of the system function for the prevention of the emergency core cooling criteria), at least one out of four high pressure safety injections is required for the primary-side leak compensation. Because the primary-side borated water supplies (borated water storage tank) are limited, the leak must be stopped timely. The damaged steam generator has to be identified and isolated and the set-point of steam generator pressure limitation has to be increased (by increasing the actuation pressure of the steam release and the main steam safety valves in the loop with the damaged steam generator).

The isolation is successful, if the main steam line, the feedwater line, and the let-down line of the damaged steam generator can be closed and the steam generator is not overfed. If the steam generator is overfed, an isolation failure is assumed, because the discharge head of the start-up and cooldown pumps is so high, that the main steam relief control valve will open.

A prerequisite for the isolation of the damaged steam generator is the function of the automatic secondary-side cooldown to the reduced maximum set point of the main steam pressure. For this purpose the heat has to be removed via at least one of the three intact steam generators, whereby the steam can be released via the main steam bypass system or via at least one of three main steam relief control valves of the intact steam generators. The steam generator tube leak is under control, if this prerequisite is fulfilled and

- the isolation is performed OR

- a secondary-side long-term residual heat removal is available via at least one steam generator and one relief control valve.

In the first case, the primary leak is stopped. In the second case, the primary leak can be compensated by the high pressure safety injection. With the available inventories of deionate resp. borated water the plant can be cooled down to a "subcritical cold" state.

For the described sequences it has been assumed that, as a prerequisite for the isolation, the automatic secondary cooldown to the reduced maximum set point of the main steam pressure was successful. However, the isolation is necessary also if the automatic secondary-side cooldown fails, e.g. because neither the main steam bypass system is available nor the three steam relief control valves in the loops of the intact steam generators open. According to the operation manual, the defect steam generator has to be isolated, if its water level reaches 15 m. Because in the considered event sequence the emergency core cooling criteria have been met (due to a failure of the system function for the prevention of the emergency core cooling criteria) and, therefore, a high pressure safety injection is activated, it has to be assumed that the water level will exceed this value. If the isolation ("late isolation") is successful and if the heat can be removed via one of the three intact steam generators and one of the three main steam safety valves, this sequence is considered to be under control due to the supply with demineralized water (for more than 10 h).

- **Sequences with successful system function for the prevention of the emergency core cooling criteria**

If the system function for the prevention of the emergency core cooling criteria is successful, the requirements for the isolation of the damaged steam generator are less demanding than described above. Increasing the set values of the steam generator pressure limitation is not necessary in this case. With respect to the system functions

- automatic secondary-side cooldown to the reduced maximum set point of the main steam pressure and
- secondary-side long-term residual heat removal

the same minimum requirements apply as for sequences with the emergency core cooling criteria being met. A high pressure safety injection for primary leak compensation is required only if both of these system functions fail. In this case, the steam gen-

erator tube leak can be controlled by "late isolation" and heat removal via one of the three intact steam generators and one of the three main steam safety valves. The requirement for the isolation (water level in the defect steam generator ≥ 15 m) is given as soon as the borated water inventories of the volume control system have been consumed and the leak is compensated by the high pressure safety injections. For the leak compensation at least one of the four injections is required.

- **Transition from the initiating event to system damage states**

The probability of the transition from the initiating event to a system damage state is $8.5 \cdot 10^{-5}$. With a frequency of $2.3 \cdot 10^{-3}/a$ for the occurrence of a steam generator tube leak, 1 - 6 cm² (see section 5.1.1), this results in a frequency of $2.0 \cdot 10^{-7}/a$ for system damage states.

- **Characteristics of the system damage states**

The system damage states are characterized by medium pressure in the primary circuit. For approx. 83 % of the sequences, time windows of more than 10 h are available; for about 17 % of the system damage states the time window is reduced to 2 to 3 h. In the first case, the system damage states are induced by failures of secondary-side safety functions (failure to isolate the damaged steam generator and loss of the long-term residual heat removal). In the second case, failures of primary-side systems (failure of the high pressure injection with the emergency core cooling criteria actuated) are concerned.

- **Contributions of system function failures**

Failures to isolate the damaged steam generator in combination with a failure of the long-term residual heat removal contribute 83 % to the frequency of system damage states. The remaining 17 % are caused by event sequences with a failure to prevent an actuation of the emergency core cooling criteria and a failure of the high pressure injections.

The isolation of the damaged steam generator fails mainly because of a failure of the main steam isolation valve (failure to close) in the damaged loop (approx. 60 %) or by a failure of the manual actions required for the isolation (approx. 40 %). A failure of the

long-term residual heat removal via the secondary side is caused mainly by the CCF of all four steam relief control valves.

The emergency core cooling criteria are actuated, first of all because the pressurizer spraying fails (check valve in the auxiliary spray line fails to open) or because the main steam bypass system opens too fast due to a failure of the main steam bypass system control. The high pressure injection required in these cases fails mainly due to failures of the high pressure safety injection pumps to run and failures of the primary isolation valves in the emergency core cooling system (see section 5.2.1).

- **Contributions of individual failure causes (importances)**

The frequency of system damage states is dominated to 70 % by failure combinations with CCF of all four main steam relief control valves (loss of the long-term residual heat removal). The failure to close of the main steam isolation valves in the main steam line of the damaged steam generator contributes 37 %, the failure of the manual action for the isolation contributes 40 %.

The contribution of CCFs is in total 88 % and of human failures 40 %, the latter essentially concerning the measures for the isolation of the damaged steam generator.

5.2.6 Loss of preferred power

- **System functions required to cope with the initiating event**

After a loss of preferred power the residual heat can be removed via one of the four steam generators. The steam generators can be fed in operational mode by the start-up and shutdown pumps or by the emergency feedwater system. If both the operational feedwater supply and the automatic actuation of the feedwater supply by the emergency feedwater system fail, the accident can be controlled, if one emergency feedwater train is started manually, before the water level in the reactor pressure vessel drops below the upper edge of the core. After loss of preferred power one to two hours are available for this manual action. For steam release the function of at least one of the four steam relief control valves or one of the four main steam safety valves is required. In the event tree analysis for the loss of preferred power it is distinguished whether the main steam collector is available or failed due to system failures ("separation of the

main steam system“). If the main steam system is separated, the requirements to the steam generator feedwater supply and the main steam release are higher: the steam from each steam generator can be released only via the relief control valve resp. the safety valve of the corresponding main steam train. Specifically, for the loss of preferred power the following system functions are distinguished:

- Main steam collector available
- Steam generator feedwater supply if the main steam collector is available by
 - 1 out of 2 trains of the start-up and shutdown system OR
 - 1 out of 4 trains of the emergency feedwater system
- Main steam release if the main steam collector is available via 1 out of 4 relief control valves
- Steam generator feedwater supply and main steam release if the main steam collector failed by 1 out of 4 steam generators with
 - Steam generator feedwater supply by 1 out of 2 start-up and shutdown system trains or the respective emergency feedwater trains AND
 - Main steam release by the corresponding relief control valve.

The requirements to the feedwater supply comprise the injection of demineralized water into the feedwater tank by one of the two demineralized water refilling pumps.

The system function requirements are nearly the same as for the “loss of main feedwater and loss of main heat sink“ (section 5.2.9) with the restriction that for the loss of preferred power for the auxiliary electrical system additional requirements with respect to the electric power supply have to be met. For practical reasons these requirements are not listed as specific system functions, but they are modeled within the fault tree.

- **Transition from the initiating event to system damage states**

The probability of the transition from a loss of preferred power to system damage states is $5.5 \cdot 10^{-5}$. With the frequency of $2.5 \cdot 10^{-2}/a$ for the loss of preferred power (see section 5.1.1) this leads to a frequency of $1.4 \cdot 10^{-6}/a$ for system damage states induced by a loss of preferred power.

- **Characteristics of the system damage states**

The system damage states in case of loss of preferred power are characterized by high pressure in the primary circuit. For 95 % of the system damage frequencies, the time windows for prevention of a core damage state are 2 to 3 h. For the remaining 5 % only 1 to 2 h are available (see table 5.5, system damage states 6 and 7).

- **Contributions of system function failures**

The essential contribution to the system damage frequency (95 %) comes from failures of the steam generator feedwater supply. In contrast, failures of the main steam release with a contribution of 5 % play a minor role.

A loss of steam generator feedwater supply is caused by a failure of both the operational feedwater supply by the start-up and shutdown pumps and the emergency feedwater supply. For the operational feedwater supply the failure to run of the deionate refill pumps and CCFs of the low power control valves, the control valves in the deionate system (failure of deionate supply to the feedwater tank) and in the start-up and shutdown system play a dominant role. Mainly the emergency feedwater diesels and the emergency feedwater pumps (start-up failure by CCF and failure to run), the pressure level control valves and the isolation valves in the injection lines (CCFs in each case) contribute to the loss of the emergency feedwater systems. A CCF of all 48 V batteries of the emergency power system 2 leads to a failure of the automatic actuation of both the emergency feedwater diesels of the emergency power system 2 and of the reactor protection signals and their respective release signals. In this situation the emergency feedwater diesels of the emergency power system 1 will not be started and the operational feedwater supply by the start-up and shutdown pumps and the feedwater supply by the emergency feedwater system fail. The contribution to the failure of the steam generator feedwater supply is approx. 16 %. Other failures of the electric power supply do not play a noteworthy role.

The main steam release fails nearly exclusively due to CCF, whereby the CCFs of the four relief control valves and of the four safety valves with 75 % deliver the highest contributions. The remaining 25 % result mainly from failure combinations with CCF of the four relief control valves and CCF of the solenoid control valves of the safety valves resp. CCF of the safety valves (main valves).

- **Contributions of individual failure causes (importances)**

The main contributions to the frequency of system damage states for a loss of preferred power come from CCFs of all four control valves (particularly pressure level control valves of the emergency feedwater system and low-load control valves), CCFs of the emergency feedwater diesels and pumps, failures to run of the demineralized water injection pumps, and the CCF of all 48 V batteries of the emergency power system 2.

CCFs in total contribute 95 % to the frequency of system damage states. Nearly one half (44 %) is induced by failure combinations containing exclusively CCFs, the higher contribution (51 %) comes from combinations of CCFs and independent failures.

Failures of manual actions do not play a role for the result.

5.2.7 Loss of main feedwater without loss of main heat sink

- **System functions required to cope with the initiating event**

In contrast to the initiating events "loss of preferred power" (see section 5.2.6) and "loss of main feedwater and loss of main heat sink" (see section 5.2.9) for this event the main heat sink (main steam bypass system) can be used for the main steam release. The further system function requirements are the same as for a loss of preferred power. Specifically, for a "loss of main feedwater without loss of main heat sink" the following system functions are distinguished:

- Main steam collector available
- Steam generator feedwater supply if the main steam collector is available by
 - 1 out of 2 trains of the start-up and shutdown system OR
 - 1 out of 4 trains of the emergency feedwater system
- Main steam release if the main steam collector is available.
 - Main steam-bypass system OR
 - 1 out of 4 relief control valves
- Steam generator feedwater supply and main steam release if the main steam collector failed via 1 out of 4 steam generators with

- Steam generator feedwater supply by 1 out of 2 trains of the start-up and shutdown system or the respective train of the emergency feedwater system AND
- Main steam release by the corresponding relief control valve.

The requirements to the feedwater supply comprise the supply of demineralized water into the feedwater tank by one out of two demineralized water injection pumps, if the main heat sink fails in the course of the transient (main steam bypass system fails to open or failure of the main steam collector).

- **Transition from the initiating event to system damage states**

The probability of the transition from the initiating event to system damage states is $1.9 \cdot 10^{-5}$. With a frequency of the “loss of main feedwater without loss of main heat sink” (see section 5.1.1) of $1.2 \cdot 10^{-1}/a$ the frequency of system damage states is $2.2 \cdot 10^{-6}/a$.

- **Characteristics of system damage states**

As for the “loss of preferred power“, the system damage states from a “loss of main feedwater without loss of main heat sink“ are characterized by high pressure in the primary circuit with – now nearly exclusively - time windows of 2 to 3 h for the prevention of a core damage state (see table 5.5, system damage state 7). The probability of transition from the initiating event to the system damage state 7 is only half of that in case of “loss of preferred power“. This can be explained by the lower requirements to the steam generator feedwater supply resp. the electric power supply (this will be explained below in some detail).

- **Contributions of system function failures**

The frequency of a system damage frequency results nearly completely from failures of the steam generator feedwater supply. In contrast, failures of the main steam release do not play a role for the result. This can be explained by the fact, that in contrast to the operational transients with a loss of the main heat sink (e.g. the “loss of preferred power“) the main heat sink can be used.

As for the “loss of preferred power”, the loss of steam generator feedwater supply can be caused both by a the loss of the operational feedwater supply by the start-up and shutdown pumps and by a loss of feedwater supply by emergency feedwater system. The loss of the steam generator feedwater supply due to a CCF of batteries is not important for the “loss of main feedwater without loss of main heat sink“. Furthermore, in contrast to the “loss of preferred power“ (and in general to the operational transients with loss of the main heat sink) the failure of the injection of demineralized water into the feedwater tank is of minor importance (operational injection). In case of a “loss of main feedwater without loss of main heat sink“ the injection of demineralized water is required, only if the main heat sink fails during the transient and the main steam is dumped to the atmosphere. These differences to the “loss of preferred power“ explain the higher availability of the steam generator feedwater supply.

The main contributions to the loss of the operational steam generator feedwater supply come from CCFs of the low-load control valves, CCFs and independent failures of the pressure level control valves of the start-up and shutdown system, and from the failure to start the start-up and shutdown pumps. The steam generator feedwater supply via the emergency feedwater system fails mainly due to CCF of the control valves for pressure level control, failures to start (CCF) and failures to run the emergency feedwater diesels and emergency feedwater pumps and due to CCF of the isolation valves in the feedwater lines.

- **Contributions of individual failure causes (importances)**

In total, the highest contributions of individual failure causes to the frequency of system damage states come from CCF of the low-load control valves (35 %), CCF of the pressure level control valves of the emergency feedwater system (29 %), CCF with start-up failures of the emergency feedwater diesels (26 %) and CCF with start-up failures of the start-up and shutdown pumps (16 %).

CCF in total contribute 97 % to the result for the frequency of system damage states and, thus, dominate the result like for the “loss of preferred power“. As for the “loss of preferred power“ and other anticipated transients, failures of manual actions do not play a role for the result.

5.2.8 Loss of main heat sink without loss of main feedwater

- **System functions required to cope with the initiating event**

Equivalent to the anticipated transients treated before, for a loss of main heat sink without loss of main feedwater the following system functions are distinguished:

- Main steam collector available
- Steam generator feedwater supply if the main steam collector is available via
 - 1 out of 3 trains of the main feedwater system (low-load) OR
 - 1 out of 2 trains of the start-up and shutdown system OR
 - 1 of 4 trains of the emergency feedwater system
 - Main steam release if the steam collector is available via 1 out of 4 release valves
- Steam generator feedwater supply and main steam release if the main steam collector failed via 1 out of 4 steam generators with
 - Steam generator feedwater supply by 1 out of 2 trains of the start-up and shutdown system or by the respective train of the emergency feedwater system AND
 - Main steam release via the corresponding relief control valve

The requirements to the feedwater supply comprise the injection of demineralized water into the feedwater tank by one the two demineralized water injection pumps.

- **Transition from the initiating event to system damage states**

The probability of the transition from a "loss of main heat sink without loss of main feedwater" to system damage states is $4.3 \cdot 10^{-5}$. With a frequency of the initiating event of $3.8 \cdot 10^{-2}/a$ (see section 5.1.1) this leads to frequency of $1.6 \cdot 10^{-6}/a$ for a system damage induced by a "loss of main heat sink without loss of main feedwater".

- **Characteristics of the system damage states**

As for the anticipated transients treated before the system damage states are characterized by high pressure in the primary circuit. Similar to the "loss of preferred power",

for 94 % of the cases (occurrence of a system damage state) the time windows for the prevention of a core damage state are 2 to 3 h, for the remaining 6 % they are 1 to 2 h (see table. 5.5, system damage states 6 and 7).

- **Contributions of system function failures**

94 % of the system damage frequencies are induced by failures of the steam generator feedwater supply. Failures of the main steam release, with 6 %, play only a minor important role for the result.

The failure combinations leading to the failure of the steam generator feedwater supply are largely the same as for a “loss of preferred power“ (see section 5.2.6) with the following modifications: For a “loss of main heat sink without loss of main feedwater“ failures of components for the electric power supply (in particular the CCF of batteries) are insignificant. Because the main feedwater pumps continue to operate after occurrence of the initiating event, failures of the start-up- and shutdown systems are of low importance. On the other hand, failure combinations with CCF of the full-load control valves (failure to close) deliver an additional contribution. Because the main feedwater pumps run, the full-load control valves have to close in order to prevent a steam generator overfeeding. The loss of a full-load control valve (failure to close) leads to an overfeeding of the respective steam generator and an isolation of the operational feedwater supply by the main feeding system and the start-up and shutdown system.

A failure of the main steam release can be caused by the same failure combinations as for a “loss of preferred power“ (see section 5.2.6.).

- **Contributions of individual failure causes (importances)**

In total, mainly the following failure causes contribute to the frequency of a system damage state: CCFs of the pressure level control valves of the emergency feedwater system (28 %), CCFs with failure to start the emergency feedwater diesels (24 %), failure to run the demineralized water injection pumps (21 %), and CCF of the low-load and full-load control valves (failure to close), each with 16 %.

As for the other anticipated transients, the contribution of CCFs to the system damage frequency is high (94 %), while failures of manual actions do not deliver a noteworthy contribution.

5.2.9 Loss of main feedwater and loss of main heat sink

- **System functions required to cope with the initiating event**

As for a “loss of preferred power“, the main feedwater and the main heat sink are not available for the secondary-side residual heat removal. The lower requirements to the electric power supply in case of “loss of main feedwater and loss of main heat sink“ are taken into account in the fault tree. The further system function requirements are the same as for a loss of preferred power. The following system functions are distinguished:

- Main steam collector available
- Steam generator feedwater supply if the main steam collector is available by
 - 1 out of 2 trains of the start-up and shutdown system OR
 - 1 out of 4 trains of the emergency feedwater system
- Main steam release if the steam collector is available via 1 out of 4 relief control valves
- Steam generator feedwater supply and main steam release if the main steam collector failed via 1 out of 4 steam generators with
 - Steam generator injection by 1 out of 2 trains of the start-up and shutdown system or the respective train of the emergency feedwater system AND
 - Main steam release via the corresponding relief control valve

The requirements to the feedwater supply comprise the injection of demineralized water into the feedwater tank by one of the two demineralized water injection pumps.

- **Transition from the initiating event to system damage states**

The probability of the transition from a “loss of main heat sink and loss of main feedwater“ to system damage states is $3.7 \cdot 10^{-5}$. With the frequency of the initiating event of

$7.5 \cdot 10^{-3}/a$ (see section 5.1.1) this leads to a frequency of $2.9 \cdot 10^{-7}/a$ for a system damage state induced by a “loss of main heat sink and loss of main feedwater“

- **Characteristics of the system damage states**

As for the anticipated transients treated before, the system damage states are characterized by high pressure in the primary circuit. Similar to a “loss of preferred power“ and a “loss of main heat sink without loss of main feedwater“, for 94 % of the cases (occurrence of a system damage state) the time windows for the prevention of a core damage state are 2 to 3 h, for the remaining 6 % they are 1 to 2 h (see table 5.5, system damage states 6 and 7).

- **Contributions of system function failures**

94 % of the system damage state frequency are induced by failures of the steam generator feedwater supply. Failures of the main steam release play only a minor role with 6 %.

The failure combinations leading to a failure of the steam generator feedwater supply are largely the same as for a “loss of preferred power“ (see section 5.2.6) with the modification that for a “loss of main heat sink and loss of main feedwater“ failures of components for the electric power supply (in particular a CCF of the batteries) do not play a role. For this transient, the unavailability of the steam generator feedwater supply is marginally lower.

The same failure combinations as for a “loss of preferred power“ lead to a loss of the main steam release (see section 5.2.6).

- **Contributions of individual failure causes (importances)**

In total, mainly the following failure causes contribute to the frequency of system damage states: CCF of the pressure level control valves of the emergency feedwater system (28 %), CCF with a failure to start the emergency feedwater diesels (24 %), failure to run the demineralized water injection pumps (21 %), and CCF of the low-load and the full-load control valves (failure to close) each with 16 %.

As for the other anticipated transients, the contribution of CCFs to the system damage frequency is high (93 %), while failures of manual actions do not contribute significantly. The contribution of CCFs comprises combinations with CCFs exclusively (36 %) and combinations of CCFs and independent failures (57 %).

5.2.10 Main steam line break outside the containment

- **Required system functions to cope with the initiating event**

The break of a main steam line is assumed for a location downstream of the main steam isolation valves. The accident is under control, if at least two steam generators can be isolated from the leak and the steam generator feedwater supply and the main steam release of at least one isolated train are available. Due to the shutdown signal for the main feedwater pumps caused by the pressure drop in the main steam system the main feedwater supply is not available. The steam generator is isolated by closing the respective main steam isolation valve. The event sequences are distinguished by to the number of the isolated steam generators.

If exactly one main steam isolation valve fails, the operational feedwater supply (start-up and shutdown system) will be blocked by reactor protection signals (due to the pressure drop in the affected steam generator). To cope with the accident, in this case the feedwater supply to at least one of the isolated steam generators by the emergency feedwater system and the main steam release from a fed steam generator are required.

If exactly two main steam isolation valves fail, the feedwater supply and the main steam release can be performed in a controlled manner via the isolated steam generator or in an uncontrolled manner via the "open" steam generators.

The failure to isolate three or four steam generators is not further analyzed and considered as system damage state.

Specifically, the following system functions are distinguished:

- Isolation of the main steam line of all steam generator
(closure of 4 out of 4 main steam isolation valves)

5 Level 1 PSA for power operation

- Steam generator feedwater supply and main steam release via 1 out of 4 trains.
Feedwater supply via 1 out of 2 trains of the start-up and shutdown system or 1 out of 4 trains of the emergency feedwater system, main steam release via 1 out of 4 relief control valves/safety valves.
- Isolation of the main steam lines of three steam generators (closure of three main steam isolation valves)
 - Steam generator feedwater supply and main steam release via 1 out of 3 trains.
Feedwater supply via 1 out of 3 trains of the emergency feedwater systems.
Main steam release: 1 out of 3 relief control valves/safety valves.
- Isolation of the main steam lines of two steam generators (closure of two main steam isolation valves)
 - Steam generator feedwater supply and main steam release via 1 out of 2 trains with isolated steam generators. Feedwater supply via 1 out of 2 trains of the emergency feedwater systems. Main steam release via 1 out of 2 relief control valves/safety valves OR
 - Steam generator feedwater supply and main steam release via 1 out of 2 trains with open steam generators. Feedwater supply via 1 out of 2 trains of the emergency feedwater system.

- **Transition from the initiating event to system damage states**

The probability of the transition from a “main steam line break outside the containment” to system damage states is $8.1 \cdot 10^{-4}$. With the initiating event frequency of $1.6 \cdot 10^{-4}/a$ (see section 5.1.1) this leads to frequency of $1.3 \cdot 10^{-7}/a$ for a system damage state induced by a “main steam line break outside the containment”.

- **Characteristics of the system damage states**

As for the transients treated before, the system damage states are characterized by high pressure in the primary circuit. Dominant are those event sequences, for which three or four steam generators cannot be isolated. The resulting system damage states are not further analyzed. However, time windows of more than 2 h are expected.

- **Contributions of system function failures**

Main contributions to the frequency of system damage states come from failures to isolate three or four steam generators. Failures of the steam generator feedwater supply and failures of the main steam release play a minor role.

CCFs of the magnetic control valves and of the main valve of the main steam isolation valves are the essential contributors to a failure of the isolation of several steam generators.

- **Contributions of individual failure causes (importances)**

In total, mainly the following failure causes contribute to the frequency of system damage states: CCF of the magnetic control valves (45 %) and of the main valves (37 %) of the main steam isolation valves, and independent failures of the main valves (14 %).

The total contribution of CCFs is 88 %, the contribution of failures of manual actions is negligible. The CCF-contribution is mainly composed of combinations with CCF alone (81 %) and combinations of CCF and independent failures (7 %).

5.2.11 Main feedwater line break outside the containments

- **System functions required to cope with the initiating event**

The main feedwater line break is assumed to occur on the discharge side of a main feedwater pump between the check valve downstream of the pump and the pump discharge side valve in one of the three trains of the main feedwater system. These parts of the lines are the most unfavorable location with respect to the control of the initiating event. As for the anticipated transients, at least one steam generator must be supplied with feedwater, and the steam must be released via at least one main steam release valve or one main steam safety valve. The operational feedwater supplies by the main feedwater system resp. by the start-up and shutdown system are not available due to the break of the main feedwater line. The feedwater supplies by the emergency feedwater system and the main steam release are efficient only for those steam generators, which on the feedwater side are isolated from the leak.

For the isolation of a steam generator, the reflux check function of the check valve in the feedwater line upstream of the steam generator or the automatic closure function of other valves is required. For the event sequences it is first distinguished, whether all four steam generators are isolated from the feedwater lines by their respective check valves or if a check valve fails. In the first case the transient can be controlled, if one of four steam generators is fed by the emergency feedwater system and if the steam is released via one of four relief control valves resp. safety valves (if the main steam collector is not available the steam has to be released from the fed steam generator, see anticipated transients). If in the second case at least at one steam generator the check valve fails (failure to close), the affected steam generator can be isolated by an automatic closure (by reactor protection signals) of the feedwater lines (full-load and low-load trains). Because in this case also the main steam isolation valves will be closed by reactor protection signals, the main steam collector is not available. For the event tree analysis, it is further distinguished, in how many redundant trains not only the check valve at the steam generator, but also the isolation of the feedwater lines and thus the isolation of the steam generator fails. If not more than two steam generators fail by isolation failure, a steam generator feedwater supply and a main steam release via at least one of the remaining trains are required to cope with the initiating event. If the isolation fails for three or four steam generators, pessimistically a system damage state is assumed. Specifically, the following system functions are distinguished:

- Isolation of all four steam generator at the feedwater side by the check valves in the main feedwater lines close to the steam generators
 - Main steam collector available
 - Steam generator feedwater supply via 1 out of 4 trains of the emergency feedwater system
 - Main steam release via 1 out of 4 relief control valves resp. 1 out of 4 safety valves

- Isolation of three steam generators at the feedwater side by the check valves in the feedwater lines close to the steam generators
 - Isolation of the fourth steam generator at the feedwater side by closure of valves in the main feedwater line
 - If four steam generators are isolated: steam generator feedwater supply and main steam release by 1 out of 4 trains (emergency feedwater system, 1 out of 4 relief control valves/safety valves)

- If three steam generators are isolated: steam generator feedwater supply and main steam release by 1 out of 3 trains (emergency feedwater system, 1 out of 3 relief control valves/safety valves)
- Isolation of two steam generators at the feedwater side by the check valves in the feedwater line close to the steam generators
 - Isolation of the third and fourth steam generator at the feedwater side by closure of valves in the feedwater line
 - If four steam generators are isolated: steam generator feedwater supply and main steam release by 1 out of 4 trains (emergency feedwater system, 1 out of 4 relief control valves/safety valves)
 - If three steam generators are isolated: steam generator feedwater supply and main steam release by 1 out of 3 trains (emergency feedwater system, 1 out of 3 relief control valves/safety valves)
 - If two steam generators are isolated: steam generator feedwater supply and main steam release by 1 out of 2 trains (emergency feedwater system, 1 out of 2 relief control valves/safety valves)

- **Transition from the initiating event to system damage states**

The probability of the transition from the initiating event to system damage states is $1.1 \cdot 10^{-3}$. With the frequency of the initiating of $2.6 \cdot 10^{-4}/a$ (see section 5.1.1) this leads to a frequency of $2.9 \cdot 10^{-7}/a$ for a system damage state induced by a “break of a main feedwater line outside the containment”.

- **Characteristics of the system damage states**

As for the anticipated transients treated before, the system damages are characterized by high pressure in the primary circuit. The time windows for the prevention of core damage states are in nearly all cases close to 2 - 3 h (see table 5.5, system damage state 7).

- **Contributions of system function failures**

Practically 100 % of the system damage frequency result from failures of the steam generator feedwater supply. Failures of the main steam release and failures to isolate three or four steam generators do not play a role for the result.

Because after a break of a main feedwater line the operational feedwater supplies (main feedwater system, start-up and shutdown system) in the area of the affected piping are not available, failures of feedwater supply by the emergency feedwater system lead to a failure of the steam generator feedwater supply.

- **Contributions of individual failure causes (importances)**

The main contributions result from CCFs of the emergency feedwater diesels resp. pumps (32 %), failures to run of the emergency feedwater diesels resp. pumps (22 %) and CCFs of valves in the emergency feedwater system (16 %).

CCFs contribute 68 % to the frequency of system damage states, failures of manual actions are insignificant for the result. The CCF contribution comprises combinations with CCFs alone (57 %) and combinations of CCFs and independent failures (11 %).

5.2.12 Synopsis of the results for system damage states

The total frequency of system damage states from plant internal initiating events is $8.2 \cdot 10^{-6}/a$. The subjective probability distribution calculated in the uncertainty analysis is discussed in section 5.4.

In the following, characteristic parameters of the most frequent system damage states and the contributions from the initiating events, from the failures of system functions, and from individual failure causes are described (see tables 5.5 and 5.6 and figure 5.1). The transition from system damage states to core damage states is treated in section 5.3. Section 5.2.13 contains estimations for those initiating events, which have not been analyzed in detail due to their low significance for the frequency of core damage states and for the level 2 of the PSA.

- **Contributions of the initiating events**

The highest contributions to the total system damage frequency result from the anticipated transients (approx. 70 %) and from the small leak at a main coolant line resp. from the small leak at the pressurizer (approx. 24 %). The highest individual contributions result from the anticipated transients "loss of main feedwater without loss of main heat sink" (27 %), "loss of main heat sink without loss of main feedwater" (22 %), from the "loss of preferred power" (17 %), and from a "small leak at a main coolant line, 2 - 25 cm²" (16 %).

- **Contributions of system function failures to the transition from initiating events to a system damage state**

The system damage states resulting from uncontrolled event sequences induced by anticipated transients in each case are dominated to more than 90 % by the loss of the steam generator feedwater supply. Thereby, the contribution of CCFs to the system unavailability is high. Failures of the operational feedwater supply are caused in essence by CCFs of valves in the main feedwater system resp. the start-up and shut-down system. Failures of the emergency feedwater system, which is redundant to the operational steam generator feedwater supply, result mainly from the CCF of the emergency feedwater diesels and of valve failures by CCF. For the "loss of preferred power" the CCF of all 48 V batteries of the emergency power system 2 contributes with approx. 16 % to the unavailability of the systems. A failure of these batteries leads to a failure of the automatic start of the emergency feedwater diesels of the emergency power system 2 and of the emergency power diesels of the emergency power system 1. Human failures are insignificant for system damage states induced by anticipated transients.

The frequency of system damage states in case of LOCAs comes to approx. 67 % from primary-side failures, to approx. 23 % by secondary-side failures and to approx. 7 % from primary-side and secondary-side failures. The primary-side failures essentially are characterized by a failure of the emergency core cooling in sump recirculation mode. Besides CCFs also independent failures of the water level measurements in the cell coolers play here an essential role. These measurements, which are required for the functioning of a safety installation, do not meet the requirements for measurements in

the reactor protection system with respect to the design (single channel) and to the test interval (yearly).

Failures of the secondary-side system functions are dominated by failures of the steam generator feedwater supply. For system damage states, caused by failures on the secondary-side and on the primary-side, failures of the main steam release for the 100K/h-cooldown and the failure to switch the high pressure safety injections from borated water storage tank suction to sump recirculation mode play the essential role. For the failure of the main steam release, failure combinations with CCF of the relief control valves are essential. These valves are required, if the main steam bypass system is not available, whereby - besides a failure of the main steam bypass system itself (fails to open) - mainly failures of the operational steam generator feedwater supply, leading to a closure of the main steam bypass system by the condenser protection, play a role. The failure of manual actions required for switching to sump recirculation mode and - failures to run of the high pressure safety injection pumps are the main contributors to the failure of high pressure safety injection in sump recirculation mode. For these pumps regular in-service inspections representative for the requirements in sump recirculation mode (with the low pressure pumps as pre-pumps) are not performed .

- **Contributions of individual failure causes (importances)**

For system damage states induced by the initiating event "small leak at a main coolant line, 2 - 25 cm²" the contribution of CCFs is approx. 73 %, none of the individual CCF combinations contributing more than 10 %. In total CCFs of valves are at the top, followed by CCFs of the measurement value logging and CCFs of pumps. Human failures bring a contribution of approx. 8 %, the measures required in case of a failure of the automatic 100 K/h cool down playing the essential role.

79 % of the system damage states are connected with high pressure (> 10 MPa) in the primary circuit. About 14 % of the event sequences lead to a system damage state with a pressure below 1 MPa, for the remaining approx. 7 % the pressure in the primary circuit is between 1 and 10 MPa.

Failures of the feedwater supply contribute 74 % to the frequency of system damage states. In these cases, CCFs of the low-load control valves (failure to open) and failures of the injections by the start-up and shutdown trains in combination with CCFs of

the emergency feedwater diesels or valves of the emergency feedwater system play the essential role.

17 % of the system damage state frequency result from failures of the low pressure or high pressure injections in case of LOCAs. The failure of the emergency core cooling in sump recirculation mode induced by failure combinations with independent failures and CCFs of the measurement value logging for the water level of the cell coolers contribute more than a half.

In total CCFs bring a contribution of 87 % to the system damage state frequency. In contrast, human failures are of minor importance with a contribution of 3 %.

Table 5.6 shows that in the most cases the unavailability of the systems is caused predominantly, in some cases even nearly completely, by common cause failures. For systems with highly reliable components and a high degree of redundancy, the probability of system failures is unavoidably dominated by CCFs.

Only few observations are available as a basis for the calculation of CCF probabilities. These observations predominantly come from the operating experience with other German, and with foreign, nuclear power plants and only in two cases from the reference plant GKN 2. The CCF probabilities are all based on judgments, performed by several experts, of the observed events and of the transferability of the events from other plants to the reference plant.

Table 5.6 also shows that human failures play a noteworthy role only for the “small leak at a main coolant line, 2 - 25 cm²” and the “steam generator tube leak, 1 - 6 cm²”. For the frequency of system damage states from a small leak at a main coolant line, 2 - 25 cm², the manual actions for plant cool down are important, which are required if the automatic 100K/h-cooldown fails. For the steam generator tube leak the manual actions for isolating the damaged steam generator play an essential role.

5.2.13 Estimations concerning initiating events not analyzed in detail

For system damage states caused by a “main steam line break outside containment” a frequency of $1.3 \cdot 10^{-7}/a$ was calculated (see section 5.2.10). Nearly 100 % of the system damage states are characterized by the failure of the isolation of three or four steam generators at the steam line side. Detailed investigations of the transition into a core

damage state were not feasible in this PSA. Even if it is assumed as an upper limit that the system damage state leads to a core damage state with a probability of 1, this initiating event gives only a contribution of approx. 5 % to the total core damage frequency.

The frequency of a system damage state caused by a “break of a feedwater line outside the containment“ is $2.9 \cdot 10^{-7}/a$. For this result, only the system damage state no. 8 resp. the loss of the steam generator feedwater supply play a role. The initiating event in total contributes approx. 5 % to the system damage frequency. In order to prevent a core damage state, the accident management measures “secondary-side bleed and feed“ (SBF) and “primary-side bleed and feed“ (PBF) can be performed. For SBF, however, the inventory of the feedwater tank is not available, and the inventory of the feedwater lines is only partially available. Therefore the time window for SBF (injection by mobile pump) is smaller than for anticipated transients. The frequency of a core damage state is estimated to be approx. $1 \cdot 10^{-8}/a$.

The consequences concerning radionuclide releases for core damage states induced by the initiating events, which have not been further analyzed, are assessed to be similar to the consequences for core damage states induced by anticipated transients. The neglected contributions to the frequency of the release category FKA are $< 1.3 \cdot 10^{-8}/a$ (“main steam line break outside the containment“) resp. approx. $1 \cdot 10^{-9}/a$ (“feedwater line break outside the containment“); the contributions to the categories FKC to FKJ are $< 1.2 \cdot 10^{-7}/a$ resp. $9 \cdot 10^{-10}/a$.

The neglected frequency contributions (see table 5.4) therefore are increased to the following values:

- Core damage frequency $< 2 \cdot 10^{-7}/a$
(compared to a frequency of $2.5 \cdot 10^{-6}/a$ as basis for level 2 of the PSA)
- Release category FKA $< 4 \cdot 10^{-8}/a$ (compared to $2.1 \cdot 10^{-7}/a$)
- Release category FKC to FKJ $< 2 \cdot 10^{-7}/a$ (compared to $2.3 \cdot 10^{-6}/a$)

5.3 Transition from system damage states to core damage states

5.3.1 Prevention of core damage states

By restoring a sufficient heat removal the plant can be brought from a system damage state to a safe state. Measures serving this purpose are plant internal accident management measures and repair of failed components. If the plant cannot be transferred into a safe state, a core damage state will occur. The probabilities for the transitions of system damage state to a core damage state are calculated by means of event tree and fault tree analyses. In case of a core damage state, plant internal accident management measures can be performed to mitigate the consequences of a core damage. These measures are treated in the level 2 part of the PSA (see chapter 6).

5.3.1.1 Plant internal accident management measures

The plant internal accident management measures “secondary-side bleed and feed” (SBF), “primary-side bleed and feed” (PBF) and measure to restore the electrical power supply are described in the emergency manual of the reference plant. The restoration of the electrical power supply is expected to have relatively low influence on the frequencies of core and plant damage states. Because the effort for a quantitative assessment of the accident management measures is high, this measure has been not taken into account in the systems analysis.

The accident management measure SBF is intended to restore the residual heat removal via the secondary circuit. This measure has to be actuated as soon as the water level in all four steam generators drops below four meters. It is planned, first to prepare and to perform the pressure relief of the steam generators. Afterwards, beginning at a main steam pressure < 2 MPa, the steam generators shall be passively fed by the inventory of the main feedwater systems. Finally at a further reduced pressure a long-term substitutional feedwater supply by a mobile pump using the demineralized water inventory of the emergency feedwater storage resp. from the pressurized feedwater inventory shall be established.

The accident management measure PBF is intended to keep the core covered by water and to provide residual heat removal via the primary-side injection and residual heat removal systems. By opening, and keeping open, both pressurizer safety valves and the pressurizer relief control valve, the pressure in the primary circuit is reduced to a

level below the zero discharge head of the safety injection pumps, so that these pumps can discharge. Below a primary pressure of 2,5 MPa, injection from the accumulators is performed. If the pressure drops below 1 MPa, a low pressure injection from the sump can be performed after the borated water storage tanks are empty. The sump water is led via the heat exchangers of the RHR system. The residual heat is removed via the component cooling water and the service water system.

The measure PBF has to be prepared by electrical actuation of the required components of the switching station, if the coolant temperature at core outlet exceeds 350 °C and the pressure inside the containment is more than 30 hPa above atmospheric pressure. The measure has also to be prepared, if it is evident that the accident management measure SBF, possibly started previously, is not successful. If the water level in the reactor pressure vessel drops below the value "MIN 3" or a the coolant temperature at core outlet increases to more than 400 °, the accident management measure PBF has to be started. All preceding, possibly still ongoing measures in this situation are subordinate to PBF.

For the analyses in this PSA it has been assumed that PBF is started only after the criteria for preparing PBF have been reached. For LOCAs the time period between the onset of the criteria and the point of time at which PBF has to be efficient to prevent core damage is so short that it is hardly possible to reach this goal /GRS 98/. GRS is estimating the success probability of PBF in case of LOCAs to be very low. Therefore, PBF is not taken into account for LOCAs in the systems analysis.

5.3.1.2 Repair measures

The term repair covers a wide spectrum of measures which can be performed in the short-term (e.g. exchange of fuses) or in the long-term (e.g. complete exchange of a large component).

The large number of possible repairs requires a constraint of the analyses to selected repair actions, in order to keep the effort for the analysis in justifiable limits. The estimations in this study therefore are restricted to repair actions,

- which can be performed within a few hours by the organizational units in charge,
- which follow well known practices, applied also in other contexts, and operational instructions (e.g. exchange of a defective electronic circuit board),

5 Level 1 PSA for power operation

- for which the situation for decision-making is favorable,
- for which due to the operating experience the reliability data of the component can be split into portions with and without repair, and
- which are important for the results of the PSA.

According to these selection criteria, for the following five types of components repair measures have been considered for a limited number of event sequences: emergency feedwater isolation valves, pressure level control valves of the start-up and shutdown system, start-up/shutdown pumps, oil pumps of the start-up/shutdown pump, and ventilators attached to a start-up/shutdown pump.

5.3.2 Characterization of the core damage states

If it is not possible in case of a system damage state to restore the heat removal by plant internal accident management measures and/or repair, the system damage state progresses into a core damage state. The 12 identified system damage states lead to initially 12 core damage states. Like the system damage states these core damage states are characterized by the following attributes:

- Primary-side, secondary-side or primary-side and secondary-side system functions failed,
- Pressure in the primary circuit (high, medium or low),
- Time period from the occurrence of the initiating event until the onset of core damage.

For the analyses of the accident sequences from a core damage state to a plant damage state to be carried out in the level 2 of the PSA, further information on characteristic attributes of a core damage state are needed. For example, it is important for the level 2, which amount of water is available in the containment sump in case of a core damage state. The event tree analyses for the core damage states therefore have to be further developed with regard to these attributes. Which attributes have to be considered and which core damage states can result, is explained in the following.

• Attributes for the characterization of the core damage states

The attributes of the core damage states, which have to be considered for the analyses of the level 2 of the PSA, are listed in table 5.7. For each attribute, the table shows which states have to be distinguished. For example, the attribute “pressure in the pri-

5.3 Transition from system damage states to core damage states

mary circuit" is described by the pressure ranges "high" (> 10 MPa), "medium" (between 1,0 and 10 MPa) and "low" ($< 1,0$ MPa).

A core damage state is characterized in such a way, that for each attribute - except the "containment ventilation isolation" – it is defined which attributes are valid and which not. With respect to the "containment ventilation isolation", for each core damage state the probability of the attribute "ventilation isolation fails" is given. To make the results easily reproducible and assessable numbers have been given to each core damage state.

Table 5.7 Core damage state attributes considered in level 2 of the PSA

No. Attribute, Description	
1	<p>Initiating event</p> <p>no.¹⁾ 2 small leak at MCL, 80 - 200 cm² no.¹⁾ 10 loss of preferred power</p> <p>3 small leak at MCL, 25 - 80 cm² 11 loss of MFW, MHS available</p> <p>4 small leak at MCL, 2 - 25 cm² 12 loss of MHS, MFW available</p> <p>6 small leak at pressurizer, 40 cm² 13 loss of MFW and MHS</p> <p>8 SG tube leak, 1 - 6 cm²</p>
2	<p>Type of the event sequence</p> <p>- small leak with pressure relief - transient, without pressure relief</p> <p>- small leak without pressure relief • with loss of SG feeding</p> <p>- transient with pressure relief with loss of MS pressure limitation</p>
3	<p>Availability of emergency power supply (grid 1)</p> <p>emergency power grid 1 operating</p> <p>emergency power grid 1 failed</p>
4	<p>Availability of primary-side injection</p> <p>• no injection</p> <p>only LP injection available</p> <p>HP injection available</p>
5	<p>Secondary-side heat removal (according to minimum requirements)</p> <p>operating</p> <p>failed</p>
6	<p>Containment ventilation isolation</p> <p>operating as designed</p> <p>failed</p>
7²⁾	<p>containment leakage retransfer</p> <p>Ventilation isolation as designed</p> <p>Ventilation isolation failed</p>
8²⁾	<p>Reactor annulus air extraction in case of accidents</p> <p>operating</p> <p>not operating</p>
9	<p>Pressure in the primary circuit</p> <p>high pressure (> 10 MPa)</p> <p>medium pressure (1,0 - 10 MPa)</p> <p>low pressure (< 1,0 MPa)</p>
10	<p>Amount of water in the containment sump</p> <p>Amount</p>
11	<p>Duration from the initiating event until the onset of core damage</p> <p>Time value</p>

1)	see table 5.1	MS	main steam	MHS	main heat sink
2)	not considered in Level 1	HP	high pressure	LP	low pressure
SG	steam generator	MCL	main coolant line	MFW	main feedwater

Besides the indication of the initiating event, most attributes pertain to the availability resp. the failure of system functions. The attributes “pressure in the primary circuit“, “amount of water injected into the containment sump“, and “time period from the initiating event until the onset of core damage“ are partly defined by the states of the attributes 1 to 5; in part different states can result from differing failure combinations. The following examples are given for explanation:

For an anticipated transient with failure of the steam generator feedwater supply and failure of the accident management measures SBF and PBF (described by attribute 2) the amount of water in the containment sump is known (attribute 10).

This is not true for attribute 10 in case of the event sequence “small leak at main coolant line, 2 - 25 cm² with failure of the low pressure injections“. At the onset of a core damage the primary-side injections are not available for this event sequence (described by attribute 4). To evaluate the amount of water in the containment sump (attribute 10), it has to be asked in addition, how many trains of the high pressure injections did work in the course of the accident. Due to system dependencies of the high pressure and the low pressure injections, some of the failure combinations lead to a failure of both system functions for this sequence.

The values for the attributes “time period from the initiating event to the onset of core damage“ are based on estimations /PÜT 01/.

Due to the relatively low importance for level 2 of the PSA, the attributes “containment leakage retransfer“ and “reactor annulus air extraction in case of accidents“ are not used to characterize the core damage states. Respective assumptions are made in the level 2 part of the PSA (see section 6.3.1).

- **Classification of the core damage states**

The definition of the different core damage states is based on the event tree analyses for the investigated initiating events. There were identified 50 event sequences with occurrence of a core damage state have been further developed based on core damage attributes 2 - 5 and 9 - 11 listed in table 5.7. This means that the states of the attributes 2 - 5 and 9 - 11 have been “scanned“ (equivalent to the scanning of system functions required to cope with the initiating event). Deviating from this general approach, the following simplifications have been made:

The event sequences with resp. without main steam collector distinguished in the event tree analysis for small leaks have been combined, because they are identical with respect to the defined attributes.

For small leaks with the occurrence of a core damage state due to failures of primary-side systems the state "secondary-side heat removal failed" (attribute 5) is neglected, because the probability of an additional loss of the secondary-side systems is negligible and the effects by the additional failure are estimated not to be significantly more severe.

The state "emergency power supply failed" (attribute 3, "emergency power supply") has been considered only for the initiating event "loss of preferred power", because a loss of the emergency power supply is negligible in our opinion for the other initiating events and the effects by the additional failure have been estimated not to be significantly more serious.

This procedure results in, initially, 69 different core damage states. For these core damage states point values for the frequencies have been calculated. The event trees and the fault trees have been numerically evaluated and additional estimations have been performed, if necessary. Based on the results it has been decided, which core damage states are to be considered as relevant for the level 2 of the PSA resp. which core damage states can be neglected. To keep the effort for the calculations in reasonable limits, frequency distributions have been calculated only for the relevant core damage states, which are further analyzed in level 2 of the PSA.

In this PSA, 35 core damage states have been estimated to be relevant. Together with their attributes and frequency distributions, they are the basis for further investigations of the accident sequences in level 2 and they form the interface between the levels 1 and 2 of the PSA. The evaluation of the frequency distributions is described in the following.

The contribution of the individual core damage states (denoted by the number of the core damage state) or of groups of core damage states (e.g. all high pressure cases) to the frequencies of the release categories is calculated in the level 2 of the PSA. In this way it is possible to trace back the results to the contributions to the frequencies of the release categories from system function failures, failure causes (CCF, human failure), from component failures, and from the initiating events. For the attribute "containment

ventilation isolation“ with the states “ventilation isolation operating as designed“ and “ventilation isolation failed“ a probability resp. a probability distribution for “ventilation isolation failed“ is provided for each core damage state. This means that core damage states with and without ventilation isolation are not distinguished. Therefore, the effect of the availability of the ventilation system on the frequency of individual release categories cannot be directly calculated by means from the core damage states (number), but it can be estimated by an evaluation of the states of the attributes.

- **Evaluation of the frequency distributions of the 35 relevant core damage states**

In order to be able to take into account the uncertainties of the results of the level 1 (due to the uncertainty of the input data, i.e. the reliability data) in the analyses for level 2, for the 35 core damage states, equivalent to the system damage states, frequency distributions have been calculated by Monte Carlo simulations with the computer program STREUSL developed by GRS. The frequency distributions of the core damage states have been calculated by correlation of the frequency distributions for the occurrence of the initiating events and for the unavailabilities of the system functions including plant internal accident management and repair measures. Also by Monte Carlo simulations the probability distributions of the failure of the containment ventilation isolation have been calculated (attribute 6). The Monte Carlo simulations are based each on 5.000 computer runs. For each computer run fractiles from the distributions of all reliability data have been “drawn“ and the reliability data have been calculated based on the distributions. The reliability data of each run have been applied for evaluating the frequencies (within this run) for all 35 core damage states and for the failure probability of the containment ventilation isolation. In this way, all 35 evaluations of a specific computer run are based on the same reliability data.

- **Core damage states combined for the presentation of the results**

For a simplified presentation of the results in this report, the 35 core damage states are combined to core damage states, which are characterized by the availability of the primary-side injection (attribute 4), by the pressure in the primary circuit (attribute 9), and by the time period from the initiating event to the onset of core damage (attribute 11) as follows:

- Availability of the primary-side injection after onset of core damage:

5 Level 1 PSA for power operation

- No high pressure and no low pressure injection available
 - Only low pressure injection (from the borated water storage tank resp. in sump recirculation mode) available
 - High pressure injection (from the borated water storage tank) available
- Pressure in the primary circuit:
- High pressure (HP) exceeding 10 MPa or
 - Medium pressure (MP) from 1 to 10 MPa or
 - Low pressure (LP) below 1 MPa
- Time period from the initiating event until onset of core damage:
- Less than 2 h or
 - 2 to 4 h or
 - 4 to 12 h or
 - More than 12 h

Based on these three attributes with three resp. four states each, 36 ($= 3 * 3 * 4$) different core damage states can be combined. Effectively, only the ten core damage states listed in table 5.8 have to be considered, because certain combinations of characteristic states do not occur. For example, a core damage state with low primary pressure and an available high pressure injection does not occur. Table 5.8 also shows the coordination of the combined core damage states to the 35 core damage states, representing the basis for the level 2 PSA (number 2 to 11, no. 1 designates the restored safe state).

5.3.3 Contributions of initiating events to core damage states

In the following sections, the results of the event tree and fault tree analyses for the combined core damage states of the analyzed initiating events are described. Specifically, the following topics are treated:

- Emergency resp. repair measures required to cope with the system damage states,
- Probabilities for the transition from system damage states to core damage states,
- Probabilities for the transition from the initiating event to core damage states,
- Characteristic attributes of the relevant system damage states,
- Contributions from failures of individual system functions, and

- Contributions of individual failure causes and contributions from CCFs and human failures.
- **Evaluation of the transition probabilities from system damage states to core damage states**

The transition probabilities are based on the evaluation of the 35 relevant core damage states (see section 5.3.2). Analogous to the approach for the system damage states, the unavailabilities of the system functions (taking into account accident management and repair measures) are equivalent to the transition probabilities from the initiating event to a core damage state. The transition probabilities from system damage states to core damage states are calculated by division of the transition probabilities of the core damage states and the system damage states.

Table 5.8 Summarized core damage states and correlation to the basic 35 core damage states for level 2 of the PSA

No. of core damage state ¹⁾	Summarized core damage states			No. of the basic core damage states for level 2 of the PSA
	Availability of primary-side injection	Pressure in the primary circuit	Time period until onset of core damage [h]	
2	no HP, no LP	LP	2 - 4	14, 21, 68
3	no HP, no LP	LP	4 - 12	1, 2
4	only LP	MP	< 2	12, 16, 22, 67
5	only LP	MP	2 - 4	15, 19, 23, 64
6	only LP	MP	4 - 12	10, 11
7	no HP, no LP	MP	4 - 12	61 – 63, 66
8	only LP	MP	> 12	3, 7, 9, 17, 18
9	only HP or. HP u. LP	HP	< 2	5, 8, 29, 38, 47, 56
10	only HP or HP u. LP	HP	2 - 4	24, 34, 43, 52
11	no HP, no LP	HP	2 - 4	28

1) see table 5.9 HP high pressure LP low pressure
 MP medium pressure

- **Estimation of the frequencies of the core damage states**

Equivalent to the frequencies of system damage states, the frequencies of the core damage states have been calculated by correlation of the frequency distributions for the occurrence of the initiating events and the unavailabilities of system functions (see section 5.2).

- **Estimation of the contributions of individual system functions**

In order to evaluate the contributions of the individual system functions to the frequency of a core damage state from a specific initiating event, the evaluations for the frequencies of the core damage states have been used (see section 5.2).

- **Evaluation of the contributions of individual failure causes (importances)**

For this purpose those failure combinations have been evaluated, which have been calculated separately for the initiating events (overall evaluations each with all core damage paths) (see section 5.2).

- **Tabular presentation of the results**

The results for the core damage states are summarized in the tables 5.9 to 5.12 .

Table 5.9 shows the probabilities for the transition from system damage states to the restored safe state resp. to the (combined) core damage states. The table also contains the frequencies of the core damage states.

In table 5.10 for the system damage states the main contributions to the unavailabilities of plant internal accident management and/or repair measures are shown. In addition to the plant internal accident management measures (PBF resp. SBF), the table depicts, which groups of initiating events (LOCA, transients, steam generator tube leaks) and which failures of system functions have induced the system damage state. The table further contains the contributions of the causes to the unavailabilities of these measures. It is distinguished between the following causes:

- System failures (column "ST")
- Insufficient time period between reaching the criteria for the preparation of accident management measures and the point of time, when the measures have to be effective (column "C")
- Failure of the manual actions in those cases, where the accident management measures could be performed due to requirements with respect to the status of systems and due to temporal restrictions (column "HF")

In the last column of table 5.10 the frequencies of the core damage states correlated to the system damage states and their total amount are given.

Table 5.11 contains the mean values of the probabilities for the transition from plant internal initiating events to core damage states.

The main contributions to the unavailabilities of plant internal accident management and repair measures for the initiating events are listed in table 5.12.

5.3.3.1 Small leak at a main coolant line, 80 - 200 cm²

- **Accident management measures to cope with the system damage states**

System damage states from a small leak at a main coolant line, 80 - 200 cm², are caused to 62 % by failures of the high pressure injections (see section 5.2.1). In this case, a core damage can be prevented in principle with the accident management measure PBF. For the investigations in this study it has been assumed that the measure PBF is only started as soon as the criteria for preparing PBF have been reached. In case of a LOCA, the time period between reaching the criteria and the point of time, at which PBF has to be effective for the prevention of core damage, is extremely short, so that it is nearly impossible to reach this goal /GRS 98/. The probability for a success of PBF in case of LOCA is estimated to be very low. Therefore, PBF in case of LOCA is not considered in the systems analysis for this aim.

38 % of the system damage states are induced by failures of the low pressure injection. In this context, CCFs of the water level measurements in the cell coolers of the RHR chain play an important role (see section 5.2.1). For these sequences with loss of the residual heat removal it is assumed that PBF cannot be effective due to failures of the RHR pumps.

- **Transition probabilities from system damage states to core damage states**

The probability of the transition from a system damage state to a core damage state in case of a small leak at a main coolant line, 80 - 200 cm², is 1, i.e. the core damage frequency is equal to the frequency of a system damage state with a value of $9 \cdot 10^{-8}/a$.

Transition probabilities from the initiating event to core damage states

With the frequency of a small leak at a main coolant line, 80 - 200 cm², of $9.0 \cdot 10^{-5}/a$ and the above calculated core damage frequency the probability for transition from the initiating event to a core damage state is $9.4 \cdot 10^{-4}$.

Table 5.9 Probabilities of the transition from system damages states to a restored

Restored safe state		Transition		
f [1/a]		1	2	3
		2.4E-7	2.2E-8	6.3E-8
5.7E-06		0.00	0.00	0.00

No. ²⁾	Core damage states			f [1/a]	Transition			
	Attribute A	P	t [h]		1	2	3	
						2.4E-7	2.2E-8	6.3E-8
2	no HP, no LP	LP	2 - 4	2.8E-7				
3	no HP, no LP	LP	4 - 12	8.7E-7				
4	only LP	MP	< 2	2.7E-7	1.0E+0	1.0E+0		
5	only LP	MP	2 - 4	9.5E-8				1.0E+0
6	only LP	MP	4 - 12	9.0E-8				
7	no HP, no LP	MP	4 - 12	1.6E-7				
8	only LP	MP	> 12	6.5E-8				
9	only HP or. HP u. LP	HP	< 2	3.1E-7				
10	only HP or. HP u. LP	HP	2 - 4	1.3E-7				
11	no HP, no LP	HP	2 - 4	2.2E-7				

1) see table 5.5

2) see table 5.8

A availability of primary injection

P primary circuit pressure

f frequency

HP high pressure

MP medium pressure

LP low pressure

t period up to core damage

5 Level 1 PSA for power operation

safe state and to core damage states

probabilities of system damage states (no., ¹ frequency [1/a])								
4	5	6	7	8	9	10	11	12
2.8E-7	8.7E-7	4.6E-7	5.9E-6	1.6E-7	6.5E-8	5.8E-9	2.6E-8	9.0E-8
0.00	0.00	0.33	0.94	0.00	0.00	0.00	0.00	0.00

probabilities of system damage states (no., ¹ frequency [1/a])								
4	5	6	7	8	9	10	11	12
2.8E-7	8.7E-7	4.6E-7	5.9E-6	1.6E-7	6.5E-8	5.8E-9	2.6E-8	9.0E-8
1.0E+0								
	1.0E+0							
						1.0E+0	1.0E+0	
								1.0E+0
				1.0E+0				
					1.0E+0			
		6.7E-1						
			2.2E-2					
			3.6E-2					

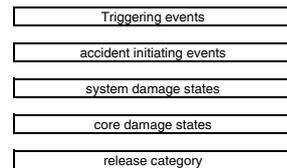
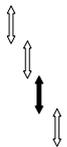


Table 5.10 Unavailabilities of plant internal accident management and repair measures

No 2)	System damage states ¹⁾				UA	Unavailabilities of plant internal repair for prevention of Main contributions Attribute
	Name/Type		t [h]	F [1/a]		
	C	P				
1	<u>PS</u>	MP	< 1	2.4E-7	1.00	LOCA, HP injection and PBF
2	<u>PS</u>	MP	1 - 1,5	2.2E-8	1.00	LOCA, HP injection and PBF
3	<u>PS</u>	MP	2 - 3	6.3E-8	1.00	LOCA, HP injection and PBF
4	<u>PS</u>	LP	2 - 4	2.8E-7	1.00	LOCA, LP injection
5	<u>PS</u>	LP	> 4	8.7E-7	1.00	LOCA, LP injection
6	<u>PS</u>	HP	1 - 2	4.6E-7	0.67	LOCA, feedwater supply and SBF and PBF T, MS pressure control/limitation and PBF
7	<u>PS</u>	HP	2 - 3	5.9E-6	0.06	T, feedwater supply and SBF and PBF
8	<u>PS</u>	MP	> 10	1.6E-7	1.00	steam generator tube leak
9	<u>PS</u>	MP	> 12	6.5E-8	1.00	LOCA, shutdown and PBF
10	<u>PS</u>	MP	2	5.8E-9	1.00	LOCA, 100K/h shutdown and HP/ LP sump suction and PBF
11	<u>PS</u>	MP	2 - 3	2.6E-8	1.00	(steam generator tube leak)
12	<u>PS</u>	MP	> 4	9.0E-8	1.00	LOCA, 100K/h-shutdown and HP/ LP sump suction and PBF
total				8.2E-6		

- 1) see table 5.5
 2) type of initiating event, system function whose failure leads to a system damage state / plant internal AM measures
- C failures cause
 P primary pressure
 MS main steam
 f frequency
 HP high pressure
 PBF primary side bleed and feed
 SBF secondary side bleed and feed

- K core damage states cannot be prevented by initiating plant internal AM measure at the criteria fixed in the emergency manual
- LOCA loss of coolant accident
 MP medium pressure
 HF human failure
 LP low pressure
 UA unavailability

5 Level 1 PSA for power operation

and the core damage frequencies of system damage states

accident management and core damage states	Contribution [%]			Core damage state frequency [1/a]	
	%	ST	K		HF
	100		100	2,4E-7	
	100		100	2,2E-8	
	100		100	6,3E-8	
	100	100	100	2,8E-7	
	100	100	100	8,7E-7	
	90		90	10	3,1E-7
	100		62	38	3,5E-7
	100	100	100	1,6E-7	
	100		100	6,5E-8	
	72		100	5,8E-9	
	100	100	100	2,6E-8	
	96		100	9,0E-8	
	In total			2,5E-6	

- P loss of primary system functions
- RBF primary side bleed and feed
- S loss of secondary system functions
- SBF secondary side bleed and feed
- ST plant internal accident management cannot be performed due to system failures
- T transients
- t periods für accident management



Table 5.11 Probabilities of the transition from initiating events to core damage states

Restored safe state		Transition probabilities		
		MCLL		
f [1/a]		2	3	4
		9.0E-5	1.5E-4	3.0E-3
0,1968		0.9991	0.9989	0.9996

Core damage states					Transition probabilities		
No ²⁾	Name/Type			f [1/a]	MCLL		
	A	P	t [h]		2	3	4
2	no HP, no LP	LP	2 - 4	2.8E-7	3.6E-4	2.9E-4	
3	no HP, no LP	LP	4 - 12	8.7E-7			3.0E-4
4	only LP	MP	< 2	2.7E-7	5.8E-4	2.0E-4	6.7E-6
5	only LP	MP	2 - 4	9.5E-8		5.1E-4	
6	only LP	MP	4 - 12	9.0E-8			3.0E-5
7	no HP, no LP	MP	4 - 12	1.6E-7			
8	only LP	MP	> 12	6.5E-8		1.0E-4	1.4E-5
9	only HP or HP and LP	HP	< 2	3.1E-7			9.1E-5
10	only HP or HP and LP	HP	2 - 4	1.3E-7			
11	no HP, no LP	HP	2 - 4	2.2E-7			

- 1) see table 5.1
 2) see table 5.8
 A availability of primary injection
 P primary pressure
 f frequency
 HP high pressure
 MCLL main coolant line leaks
 SGTL SG tube leaks

of initiating events (event group, no. ¹) frequency [1/a]						
PL	SGTL	Anticipated transients				
6	8	10	11	12	13	
8.5E-4	2.3E-3	2.5E-2	1.2E-1	3.8E-2	7.5E-3	
0.9995	0.9999	1.0000	1.0000	1.0000	1.0000	

of initiating events (event group, no. ¹) frequency [1/a]						
PL	SGTL	Anticipated transients				
6	8	10	11	12	13	
8.5E-4	2.3E-3	2.5E-2	1.2E-1	3.8E-2	7.5E-3	
2.8E-4						
2.0E-4						
2.1E-6	1.4E-5					
	7.2E-5					
		4.5E-7	1.7E-8	4.5E-7	4.5E-7	
		1.0E-6	4.6E-7	1.1E-6	1.0E-6	
		8.5E-6				

PL pressuriser leaks
 LP low pressure
 MP medium pressure
 t time period up to core damage

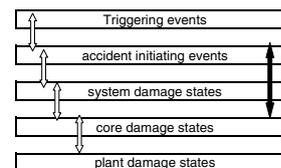


Table 5.12 Unavailabilities of system functions, plant internal accident management

No.	Initiating event ¹⁾		Unavailabilities of system functions and and repair for prevention of	
	Name/Type	f [1/a]	UA	Main contributions Attribute ²⁾
2	small leak, 80 - 200 cm ²	9.0E-5	9.4E-4	HP injection / PBF LP injection
3	small leak, 25 - 80 cm ²	1.5E-4	1.1E-3	HP injection / PBF LP injection FW supply / SBF and PBF
4	small leak, 2 - 25 cm ²	3.0E-3	4.4E-4	LP injection FW supply / SBF and PBF 100K/h-shutdown /HP /LP sump suction / PBF
6	small pressurizer leak, 40 cm ²	8.5E-4	4.8E-4	LP injection HP injection / PBF
8	SG tube leak, 1 – 6 cm ²	2.3E-3	8.6E-5	isolation and long-term RHR preventing emergency cooling crite- ria and HP – injection
10	Loss of pre- ferred power	2.5E-2	1.0E-5	FW supply / SBF and PBF MS pressure control/limitation / PBF
11	Loss of MFW without loss of MHS	1.2E-1	4.8E-7	FW supply / SBF and PBF MS pressure control/limitation / PBF FW supply / repair and PBF
12	loss of MHS without loss of MFW	3.8E-2	1.6E-6	FW supply / SBF and PBF MS pressure control/limitation FW supply / repair and PBF
13	loss of MFW and loss of MHS	7.5E-3	1.5E-6	FW supply / SBF and PBF MS pressure control/limitation / PBF FW supply / repair and PBF

1) see table 5.1

2) system function, loss of which causes system damage / plant internal accident management

SG steam generator

HF human failure

CCF common cause failures

f frequency

HP high pressure

MFW main feedwater

MHS main heat sink

C core damage states cannot be prevented for the criteria mentioned in the emergency manual in case of plant internal accident

LP low pressure

UA unavailability

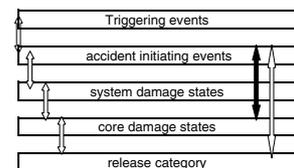
RHR residual heat removal

5 Level 1 PSA for power operation

and repair measures and core damage frequencies for initiating events

plant internal accident management core damage states					Core damage state frequencies [1/a]			
%	Contribution [%]				Failure cause			Sum
	CCF	HE	ST	C	<u>P</u> S	<u>P</u> S	<u>P</u> S	
62 38	37	2	39	100	9.0E-8			9.0E-8
62 26 8	46	1	27	100	1.4E-7	1.6E-8	4.6E-9	1.6E-7
68 21 7	73	4	67	100	8.7E-7	3.3E-7	1.1E-7	1.3E-6
58 42	59	1	54	100	4.0E-7		1.8E-9	4.0E-7
83 17	88	40	62	100	1.9E-8	1.6E-7	7.0E-9	1.8E-7
95 5	99	16	4 (SBF)	84	2.5E-7			2.5E-7
85 3 12	98	100	19 (SBF)		5.7E-8			5.7E-8
65 27 8	97	100	22 (SBF)		6.0E-8			6.0E-8
67 24 9	96	100	21 (SBF)		1.1E-8			1.1E-8
In total					1.5E-6	8.8E-7	1.2E-7	2.5E-6

- P loss of primary system functions
- PBF primary side bleed and feed
- S loss of secondary system functions
- SBF secondary side bleed and feed
- FW feedwater
- ST plant internal accident management cannot be performed due to system failures



- **Core damage states**

In case of a small leak at a main coolant line, 80 - 200 cm², the core damage states are characterized by low resp. medium pressure in the primary circuit and a time period of < 4 h until onset of core damage. The low pressure injection is available after occurrence of core damage in approx. 60 % of the cases (core damage states 2 and 4 in table 5.11).

- **Contributions of system function failures**

In case of LOCAs, system damage states result in core damage states, because PBF cannot be performed timely due to the very short time periods being available. Furthermore, in nearly 40 % of the cases of a small leak at a main coolant line, 80 - 200 cm², the system damage state is induced by a failure of the low pressure injection so that PBF cannot be performed.

- **Contributions of individual failure causes (importances)**

Besides the failure of the accident management measure PBF (due to the short time period as a consequence of the late reaching of the criteria for the preparation of PBF) with a contribution of 61 % to the core damage frequency, also independent failures of the primary isolation valves, the failure to run of the high pressure pumps, and independent failures of the water level measurements in the cell coolers play an important role (see section 5.2.1).

The total contributions of CCFs is approx. 37 %, human failures are of minor importance (see section 5.2.1).

5.3.3.2 Small leak at a main coolant line, 25 - 80 cm²

- **Accident management measures to cope with the system damage states**

With respect to system damage states with failures of the primary-side system functions (approx. 90 %) the same is true as for a small leak at a main coolant line, 80 - 200 cm² are also valid. Accident management measures (PBF) either cannot be per-

formed due to system function failures or the success probability is estimated to be low. Approx. 8 % of the frequency of system damage states result from failures of the steam generator feedwater supply, but only for part of the failure combinations the criteria for the preparation of the accident management measure SBF will be reached (water level < 4 m in all four steam generators). Furthermore, even in these cases the time period between reaching the criteria and the point of time, at which SBF must be effective, is very short, so that the probability for the success of SBF is assumed to be low. SBF is therefore not considered in the systems analysis In case of LOCA.

- **Transition probabilities from system damage states to core damage states**

In case of a small leak at a main coolant line, 25 - 80 cm², the probability of transition from a system damage state to a core damage state is 1, i.e. the core damage frequency is equal to the frequency of the system damage state with a value of $1,6 \cdot 10^{-7}/a$. In 74 % of the cases, the criteria for the preparation of accident management measures are reached too late, in the remaining 26 % accident management measures cannot be performed due to systems failures.

- **Transition probabilities from the initiating event to core damage states**

With the frequency of a small leak at a main coolant line, 25 - 80 cm², of $1,5 \cdot 10^{-4}/a$ and the above calculated core damage frequency the transition probability from an initiating event to a core damage state is $1,1 \cdot 10^{-3}$. Nearly 90 % of the frequency result from failures of the high pressure and low pressure injection.

- **Core damage states**

In case of a small leak at a main coolant line, 25 - 80 cm², most of the core damage states are characterized by medium pressure in the primary circuit (74 %). The core damage states are mainly caused by failures of the high pressure injection and the secondary-side cool down. The time period until onset of core damage in the most cases is lower than 4 h, in part the time period exceeds 12 h (if the HP sump recirculation is started), after onset of core damage only the LP injections are available in these cases. In 26 % of the core damage states, the sequence leads to core damage between 2 and 4 h after occurrence of the leak. In these cases, the pressure in the primary circuit is less than 1 MPa. Furthermore, after onset of core damage, neither HP

injections nor LP injections are available. The failure of the low pressure injection is the main cause for this core damage state.

- **Contributions of system function failures**

In case of LOCAs, all system damage states result in core damage states, because PBF cannot be performed timely due to the short available time span resp. due to system function failures. In case of a small leak at a main coolant line, 25 - 80 cm², PBF cannot be performed in 26 % of the cases due to a failure of the low pressure injection.

Attributing the results for core damage states to system function failures, besides the failure of the low pressure injection (26 %), mainly the failure of the high pressure injection (62 %) has to be mentioned. The failure of secondary-side system functions with a contribution of 12 % is of minor importance.

- **Contributions of individual failure causes (importances)**

Besides the failure of the accident management measure PBF (due to the very short time period because of the late reaching of the criteria for preparing PBF) with a contribution of 74 % to the core damage frequency, also independent failures of the primary isolation valves, the failure to run of the high pressure pumps, and independent failures of the water level measurements in the cell coolers play an important role (see section 5.2.2).

The total contribution of CCFs is approx. 37 %, human failures are of minor importance (see section 5.2.2).

5.3.3.3 Small leak at a main coolant line, 2 - 25 cm²

- **Accident management measures to cope with the system damage states**

As for the small leaks at a main coolant line, 80 – 200 cm² and 25 – 80 cm² (see sections 5.3.3.1 and 5.3.3.2), accident management measures are not taken into account. For the small leak at a main coolant line, 2 - 25 cm², the contribution to the frequency of core damage states, for which the low pressure injections are failed and thus the acci-

dent management measure PBF cannot be performed, with 68 % is higher than for the larger leaks.

- **Transition probabilities from system damage states to core damage states**

For a small leak at a main coolant line, 2 - 25 cm², the probability of transition from of a system damage state to a core damage state is 1, i.e. the core damage frequency is equal to the frequency of a system damage state with a value of $1.3 \cdot 10^{-6}/a$ (see section 5.2.3). In 68 % of the cases accident management measures cannot be performed due to systems failures, for the remaining 32 % the criteria for accident management measures are reached too late.

- **Transition probabilities from the initiating event to core damage states**

The probability of transition from the initiating event to a core damage state is $4.4 \cdot 10^{-4}$. Nearly 70 % of the frequency result from failures of the low pressure injection. The failure of the feedwater supply contributes 21 %.

- **Core damage states**

In case of a small leak at a main coolant line, 2 - 25 cm², 68 % of the core damage states have low pressure primary in the primary circuit. These are mainly core damage states resulting from a failure of the low pressure injection. For 21 % of the core damage states the pressure in the primary circuit is high. In these cases, the steam generator feedwater supply is failed. High pressure occurs only for the smaller leak cross sections (2 - 12 cm²). All other core damage states (12 %) are characterized by medium pressure in the primary circuit. The time periods from the initiating event until the onset of core damage for core damage states, which are relevant for the results, vary from less than 2 h (22 %, mainly high pressure) to 4 - 12 h (80 %) and higher (3 %). After occurrence of core damage with high pressure in the primary circuit, the high pressure injection and the low pressure injection are available, in most other cases neither high pressure injection nor low pressure injection are available.

- **Contributions of system function failures**

In case of LOCAs, all system damage states lead to core damage states, because PBF cannot be performed either due to the short available time period and/or due to system function failures. After a small leak at a main coolant line, 2 - 25 cm², PBF cannot be performed in 68 % of the cases due to the failure of the low pressure injection.

Attributing the core damage states to system function failures, besides the dominating failure of the low pressure injection (68 %), also the failure of the steam generator injection (21 %) is significant. Failures of the 100K/h-cooldown and failures of the high pressure sump recirculation are minor important with a contribution of 7 %. The causes of system function failures are outlined in section 5.2.3.

- **Contributions of individual failure causes (importances)**

Besides the failure of the accident management measure PBF (due to the short time period available by the late arising of the criteria for preparing PBF) with a contribution of 32 % to the frequency of the core damage state, also independent failures and the CCF of the water level measurements in the cell coolers of the RHR chain, and CCF of valves in the main feedwater and the emergency feedwater system play an important role (see section 5.2.3).

Failure combinations with CCF have a total contribution of approx. 73 %, human failures are minor important with a contribution of 4 % (see section 5.2.3).

5.3.3.4 Small leak at the pressurizer by stuck open safety valve

- **Accident management measures to cope with the system damage states**

As for the small leaks at a main coolant line, accident management measures are not taken into account. For a small leak at the pressurizer the contribution of those system damage states, for which the low pressure injection failed and therefore the accident management measure PBF cannot be performed, is 58 %. For the remaining 42 %, accident management measures are not taken into account due to the above mentioned reasons (see sections 5.3.3.1 and 5.3.3.3).

- **Transition probabilities from system damage states to core damage states**

In case of a small leak at the pressurizer by stuck open safety valve, the probability of transition from a system damage state to a core damage state is 1, i.e. the core damage frequency is equal to the frequency of a system damage state with a value of $4,0 \cdot 10^{-7}/a$ (see section 5.2.4). In 58 % of the cases, accident management measures cannot be performed due to systems failures, in 42 % the criteria for accident management measures arise too late.

- **Transition probabilities from the initiating event to core damage states**

The probability of transition from the initiating event to a core damage state is $4.8 \cdot 10^{-4}$, mainly resulting from failures of the low pressure injection (58 %) and the high pressure injection with failure of PBF (42 %).

- **Core damage states**

In case of a small leak at the pressurizer leak by stuck open safety valve, most core damage states (58 %) have low pressure in the primary circuit and occurrence time periods of 2 - 4 h. These are mainly core damage states resulting from a failure of the low pressure injection. The remaining cases (42 %) are characterized by medium pressure in the primary circuit and time periods below 2 h. Nearly in all of these cases, the failure of the high pressure injections leads to the core damage state. In this case, the low pressure injection is available after the onset of core damage; otherwise, an injection into the primary circuit can be performed neither with the high pressure nor with the low pressure systems.

- **Contributions of system function failures**

In case of LOCAs, all system damage states lead to core damage states, because PBF cannot be performed either due to the short available time period and/or due to system function failures. After a small leak at the pressurizer by stuck open safety valve, PBF cannot be performed in 58 % of the cases due to a failure of the low pressure injections.

Attributing the core damage states to system function failures, besides the loss of the low pressure injections (58 %), also the failure of the high pressure injections is important (42 %). The causes of system function failures are outlined in section 5.2.4.

- **Contributions of individual failure causes (importances)**

Besides the failure of the accident management measure PBF (due to the short time period by late arising of the criteria for preparing PBF) with a contribution of the 58 % to the core damage frequency, also independent failures and CCF of the water level measurements in the cell coolers of the RHR chain, independent failures of the primary isolation valves of the RHR system, and failures to run of the safety injection pumps play an important role (see section 5.2.4).

Failure combinations with CCF have a contribution of approx. 59 %, human failures are of minor importance with a contribution of 1 % (see section 5.2.4).

5.3.3.5 Steam generator tube leak, 1 - 6 cm²

- **Accident management measures to cope with the system damage states**

In case of a steam generator tube leak the criteria for performing the accident management measures SBF resp. PBF are not met (see section 5.3.1.1). Therefore these measures are not taken into account by the PSA.

- **Transition probabilities from system damage states to core damage states**

For a steam generator tube leak, 1 - 6 cm², the probability of transition from a system damage state to a core damage state is 1, i.e. the core damage frequency is equal to the frequency of a system damage state with a value of $2,0 \cdot 10^{-7}/a$ (see section 5.2.5). Accident management measures are not taken into account because the criteria are not met.

- **Transition probabilities from the initiating event to core damage states**

The probability of transition from the initiating event to a core damage state is $8.5 \cdot 10^{-5}$. It is mainly resulting from failures of the system functions "isolation of the damaged steam generator" and "long-term residual heat removal" (see section 5.2.5).

- **Core damage states**

In case of a steam generator tube leak, 1 - 6 cm², the core damage states are characterized by medium pressure in the primary circuit. In most cases (83 %), the core damage state occurs after 4 - 12 h. The high pressure and the low pressure injections are not available at that time. The causes of these core damage states are mainly failures of the system functions "isolation of the defect steam generator " and "long-term residual heat removal". Core damage states caused by actuation of the emergency core cooling criteria and the failure of the high pressure injections (17 % of the core damage frequency), are rare. In these cases, the core damage state occurs already after 2 - 4 h. The low pressure injection is available for this core damage state.

- **Contributions of system function failures**

In case of a steam generator tube leak, 1 - 6 cm², all system damage states lead core damage states, because there are no criteria for performing SBF and PBF.

Attributing the results for core damage states to failures of system functions, the following can be stated: Isolation failures of the damaged steam generator in combination with a failure of the long-term residual heat removal have a contribution of 83 % to the frequency of system damage states. The remaining approx. 17 % result from sequences, for which the actuation of the emergency core cooling criteria could not be prevented and the high pressure injection fails. Further details are outlined in section 5.2.5.

- **Contributions of individual failure causes (importances)**

Besides the "failure "of the accident management measures (no criteria for their performance), also failure combinations with failure of all four main steam relief control valves by CCF and the failure of the main steam isolation valves in the main steam line

of the damaged steam generator and the failure of the manual actions for isolating the damaged steam generator play the essential roles (see section 5.2.5).

CCF have a total contribution of 88 %, human failures - mainly for the measures to isolate the damaged steam generator – have a contribution of 40 % (see section 5.2.5).

5.3.3.6 Loss of preferred power

- **Accident management measures to cope with the system damage states**

In case of a loss of preferred power system damage states can be transferred into safe state by accident management measures and eventually by repair measures. In this PSA, the accident management measures SBF and PBF as well as repair measures for selected components have been considered (see sections 5.3.1.1 and 5.3.1.2). In order to evaluate the minimum requirements, estimations based on thermal hydraulic calculations for the „loss of main feedwater without loss of main heat sink“ (see section 5.3.3.7) have been performed. Based on the event sequences, which lead to a system damage state because of failures of design-basis system functions, the following accident management resp. repair measures are required:

- for a failure of the steam generator feedwater supply:
 - SBF (injection via mobile pump) OR
 - SBF (using the water inventory of the feedwater lines und the feedwater tank) and repair OR
 - PBF
- for a failure of the main steam release (pressure limitation): PBF

This means that with respect to SBF two different requirements are considered:

In order to prevent a core damage state a long-term steam generator feedwater supply via a mobile pump has to be established. For this purpose, measures for steam generator pressure release and for connecting the mobile pump are required, whereby at least one of the four main steam relief control valves or one of the four main steam safety valves have to be opened. The injection has to be performed via at least one of the four steam generators.

If the steam generator feedwater supply with the mobile pump cannot be started, because e.g. valves in the feedwater lines do not open, a core damage state can only be prevented by repair measures (or by PBF). As a prerequisite for successful repair, SBF has to be performed so far, that the water inventory of the feedwater tank and the feedwater lines can be used and so the time span required for the repair becomes available. For this purpose, at least two of the four main steam relief control valves must be opened, and at least two of the three main feedwater pump trains and at least four feedwater lines have to be connected.

For PBF, at least two of the three pressurizer valves must open.

- **Transition probabilities from system damage states to core damage states**

In case of a loss of preferred power, the probability of transition from a system damage state to a core damage state is 0,18. This means that 18 % of the system damage states lead to core damage states. In most cases (82 %), however, the plant can be transferred into a safe state by means of the accident management measures SBF or PBF. The major contribution of the failure of SBF and PBF results from the CCF of all 48 V batteries of the emergency power system 2, leading - on the one side - to the failure of the operational feedwater supply with the start-up and shutdown pumps and of the emergency feedwater system (see section 5.2.6), and – on the other side - complicating the performance of accident management measures. In the opinion of GRS, this situation is not sufficiently dealt with by the emergency manual.

With a frequency of $1,4 \cdot 10^{-6}/a$ for a system damage state in case of loss of preferred power (see section 5.2.6) and the probability of 0,18 for the transition, the core damage frequency in case of a loss of preferred power is $2,5 \cdot 10^{-7}/a$.

In the following, the transition probabilities from the individual system damage states in case of loss of preferred power are discussed (see section 5.2.6 as well as tables 5.5 and 5.6).

The system damage state no. 7 with 95 % has the major contribution to the frequency of system damage states in case of a loss of preferred power (see table 5.5). The system damage state results from the failure of the steam generator feedwater supply and may lead to two different core damage states (no. 10 and 11, see table 5.9) depending on the failure causes. The most frequent causes (89 %) are component failures of the

start-up and shutdown system and of the emergency feedwater system. For these cases, a probability of 0,02 for the transition from a system damage to a core damage state is calculated (core damage state no. 10). The probability of transition is dominated by the failure of the manual actions to perform SBF resp. repair measures and PBF. Approx. 16 % of the system damage frequency result from the CCF of all 48 V batteries of the emergency power system 2. In this case, system functions needed for SBF and PBF fail, i.e. the transition probability is 1. This leads to a total probability of 0.18 for the transition from the system damage state no. 7 to the core damage state no. 11.

A contribution of 5 % to the frequency of a system damage state in case of a loss of preferred power comes from the failure of the main steam pressure limitation (no. 6 in table 5.5). The probability of transition from a system damage to a core damage state in this case is 0.17, dominated by the failure of the manual actions for PBF.

- **Transition probabilities from the initiating event to core damage states**

The probability of transition from the initiating event to a core damage state is $1,0 \cdot 10^{-5}$, resulting mainly from failures of the steam generator feedwater supply and of the accident management measures SBF and PBF. 85 % of the cases are caused by the above mentioned CCF of all 48 V batteries of the emergency power system 2. The remaining 15 % are caused mainly by the pump and valve failures mentioned in section 5.2.6, which lead to a failure of the steam generator feedwater supply, and by human failures, which lead to a failure of the accident management and repair measures.

- **Core damage states**

The core damage states in case of a loss of preferred power are characterized by high pressure in the primary circuit. In most cases (96 %) the core damage state occurs after 2 - 4 h. In the remaining 4 %, resulting from failures of the main steam release and loss of the accident management measure PBF, these time periods are < 2 h. After onset of core damage the high pressure and the low pressure injections are available only in 15 % of the cases. In case of a CCF of the batteries, which has the highest contribution to the core damage frequency with 85 %, these injections fail.

- **Contributions of system function failures**

In case of a loss of preferred power, failures of the steam generator feedwater supply (leading to a system damage state) and of the accident management measures SBF and PBF play the essential role. 85 % of the core damage frequency result from the CCF of all 48 V batteries of the emergency power system 2, which - on the one side – leads to a failure of the operational feedwater supply by the start-up and shutdown pumps and by the emergency feedwater system (see section 5.2.6) and - on the other side - prevents the performance of the accident management measures. In additional 10 %, the steam generator feedwater supply is fails due to failures of pumps and valves. In these cases, human failures lead to the failure of the accident management measures SBF and PBF resp. the repair measures. For the remaining 5 % of the core damage frequency, the failure of the main steam release (main steam pressure limitation) is caused by the CCF of the main steam relief control valves and main steam safety valves. SBF cannot be performed in this case. Mainly the failure of the manual actions for performing the accident management measure lead to the failure of PBF.

- **Contributions of individual failure causes (importances)**

Mainly CCFs of all 48 V batteries of the emergency power system 2 contribute to the core damage frequency (85 %). In the opinion of GRS, this situation is not sufficiently dealt with by the emergency manual. It is assumed that in this case accident management measures will not be performed resp. are not successful. The remaining 15 % result mainly from failure combinations, which include the failure of SBF and of PBF. The failure of repair measures is of minor significance with a contribution of approx. 1 %. The importances of individual component failures leading to system damage, are all below 3 %.

CCF have a total contribution of 99 %, human failures of 16 %.

5.3.3.7 Loss of main feedwater without loss of main heat sink

- **Accident management measures to cope with the system damage states**

As for the loss of preferred power, for the loss of main feedwater without loss of main heat sink the accident management measures SBF and PBF as well as the repair of

selected components are considered. The event sequences and the minimum requirements to the system functions (SBF, PBF) are the same as for the loss of preferred power (see section 5.3.3.6). To evaluate the relevant time periods for the performance of manual actions thermo hydraulic calculations have been performed.

- **Transition probabilities from system damage states to core damage states**

In case of a loss of main feedwater without loss of main heat sink, the probability of transition from a system damage state to a core damage state is $2,5 \cdot 10^{-2}$. This means, that about 3 % of the system damage states lead to a core damage. In most cases (97 %) the plant can be transferred into a safe state by the accident management measures SBF resp. repair or PBF. The essential contribution from the failures of SBF and PBF results from the failure of manual actions for performing the measures.

With the system damage frequency of $2,6 \cdot 10^{-6}/a$ (see section 5.2.7) for a loss of main feedwater without loss of main heat sink and the above mentioned transition probability of $2,5 \cdot 10^{-2}$ the core damage frequency for a loss of main feedwater without loss of main heat sink is $5,5 \cdot 10^{-8}/a$.

In the following, the transition probabilities from the individual system damage states in case of a loss of main feedwater without loss of main heat sink are discussed (see section 5.2.7 and tables 5.5 and 5.6).

With a contribution of nearly 100 % the system damage state no. 7 dominates the result for the frequency of system damage states in case of a loss of main feedwater without loss of main heat sink (see table 5.5). This system damage state is induced by the failure of the steam generator feedwater supply and it leads to core damage state no. 10 if SBF and PBF fail (see table 5.9). The probability of transition is $2,4 \cdot 10^{-2}$. With contribution of 70 %, SBF and PBF are not available due to failures of the manual actions after a failure of the steam generator feedwater supply (start-up and shutdown system and emergency feedwater system). For the remaining 30 %, SBF fails due to valve failures. An injection by the mobile pump is not possible, if not at least one emergency feedwater line can be connected to the respective steam generator. This is the case, if e.g. none of the four emergency feedwater isolation valves opens. In this case, core damage can be prevented by repair measures or PBF. Again, mainly failures of the manual actions lead to the failure of PBF. With respect to repair, the following can

be stated: Nearly half of the contribution of 30 % come from failure combinations, in which repair was not successful, either because the required time period was not available or because of the repair measures themselves fail (failure of the manual actions). The time period required for repair is not available, if "SBF for using the water inventory of the feedwater lines and the feedwater tank" fails (failure of the manual actions). The remaining approx. 15 % are failure combinations, for which no repair measures are considered (see section 5.3.1.2).

The failure of the main steam pressure limitation (system damage state no. 6) gives a negligible contribution of less than 1 % to the frequency of system damage states (see section 5.2.8). If accident management resp. repair measures fail, the system damage state leads to the core damage state no. 9. For this sequence, neither SBF nor repair measures are expected to be successful. Therefore, a higher probability of transition from a system damage state to a core damage state (0.35) is calculated than for the above mentioned sequences with loss of the steam generator injection ($2.4 \cdot 10^{-2}$). Therefore, the core damage state no. 9 contributes 4 % to the frequency of core damage states in case of a loss of main feedwater without loss of main heat sink. The transition probability is dominated by the failure of the manual actions required for performing PBF actions.

- **Transition probabilities from the initiating event to core damage states**

The probability of transition from the initiating event to a core damage state is $4,8 \cdot 10^{-7}$ mainly resulting from failures of the steam generator feedwater supply and of the accident management measures SBF and PBF.

- **Core damage states**

The core damage states in case of a loss of main feedwater without loss of main heat sink are characterized by high pressure in the primary circuit. In most cases (96 %) the core damage state occurs after 2 - 4 h (core damage state no. 10). For the remaining 4 %, caused by failures of the main steam release and failures of the accident management measure PBF, these time periods are below 2 h (core damage state no. 9). After occurrence of a core damage the high pressure and the low pressure injections are available.

- **Contributions of system function failures**

In case of a loss of main feedwater without loss of main heat sink, failures of the steam generator feedwater supply (leading to a system damage state) and the accident management measures SBF and PBF play the essential role. The steam generator feedwater supply fails, if both injections by the start-up and shutdown system and the four injections by the emergency feedwater system fail. For the start-up and shutdown system the CCF of the low-load control valves and the pressure level control valves and the start-up failure of the start-up and shutdown pumps are the most frequent failure causes. Mainly CCFs of the pressure level control valves, failures to start (CCF) and failures to run of the emergency feedwater diesels and emergency feedwater pumps, and CCFs of the emergency feedwater isolation valves contribute to the failure of the emergency feedwater system. SBF and PBF mainly fail due to failures of the manual actions.

- **Contributions of individual failure causes (importances)**

Failures of the manual actions for PBF (100 %) and SBF (64 %) have the highest importance for the core damage frequency, followed by CCF of four low-load control valves (37 %), pressure level control valves of the emergency feedwater system (23 %), emergency feedwater diesels (21 %), pressure level control valves of the start-up and shutdown system (14 %), and CCF of the four emergency feedwater isolation valves (11 %). The contributions of all other component failures resp. failures of manual actions are below 10 %.

CCF in total contribute 98 %, human failures contribute 100 % to the core damage frequency.

5.3.3.8 Loss of main heat sink without loss of main feedwater

- **Accident management measures to cope with the system damage states**

As with the transients treated before, in case of a system damage state induced by loss of main heat sink without loss of main feedwater, core damage can be prevented by the accident management measures SBF resp. repair or PBF. The event sequences and the minimum requirements to the system functions (SBF, PBF) are the same as for

the loss of preferred power (see section 5.3.3.6). The relevant time periods for performing these manual actions have been estimated by means of the thermal hydraulic calculations for the loss of main feedwater without loss of main heat sink.

- **Transition probabilities from system damage states to core damage states**

In case of a loss of main heat sink without loss of main feedwater, the probability of transition from a system damage state to a core damage state is $3,3 \cdot 10^{-2}$. This means, that approx. 3 % of the system damage states lead to a core damage. In most cases (97 %) the plant can be transferred into a safe state by means of the accident management measures SBF resp. repair or PBF. The essential contribution from failures of SBF and PBF results from the failure of the manual actions to perform the measures.

With the frequency of a system damage state from a loss of main heat sink without loss of main feedwater of $1,8 \cdot 10^{-6}/a$ (see section 5.2.8) and the transition probability of $3,3 \cdot 10^{-2}$ the core damage frequency in case of a loss of main heat sink without loss of main feedwater is $6,0 \cdot 10^{-8}/a$.

The frequency of the system damage states is dominated by the system damage state no. 7 (95 %) with a failure of the steam generator feedwater supply. If SBF resp. repair and PBF fail, the system damage state leads to core damage state no. 10. The transition probability is $2,8 \cdot 10^{-2}$. Similar to a loss of main feedwater without loss of main heat sink, SBF and PBF fail in most cases (63 %) due to human failures. In the remaining cases (37 %), valve failures lead to the failure of SBF. The repair measures considered in this PSA (see section 5.3.1.2) fail either because the available time is too short or due to human failures (see section 5.3.3.7). Nearly 10 % of the frequency of core damage state no. 10 come from failure combinations, which contain a failure to close of a main steam safety valve (failure to close after opening). For the initiating event "loss of main heat sink without loss of main feedwater" the actuation of the main steam safety valves is expected. If a valve sticks open, the main steam collector is no longer available. In these cases, repair measures are not considered (see section 5.3.1.2). Therefore, the probability of transition from a system damage state to a core damage state with a value of $3,3 \cdot 10^{-2}$ is slightly higher than for a loss of main feedwater without loss of main heat sink ($2,4 \cdot 10^{-2}$).

The probability of transition from system damage state no. 6 (failure of the main steam pressure limitation) to core damage state no. 9 with 0.18 is the same as for the other anticipated transients (see sections 5.3.3.6, 5.3.3.7 and 5.3.3.9).

- **Transition probabilities from the initiating event to core damage states**

The transition probability from the initiating event to a core damage state is $1,6 \cdot 10^{-6}$ and results to 73 % from failures of the steam generator feedwater supply and of the accident management measures SBF and PBF. The contribution is lower than for a „loss of main feedwater without loss of main heat sink“ (97 %), because the main feedwater pumps can be used for steam generator feedwater supply. Failures of the main steam pressure limitation and failures of PBF with 27 % are more significant than for the "loss of main feedwater without loss of main heat sink" (3 %), because the main steam bypass system is not available for the main steam release in case of a „loss of main heat sink without loss of main feedwater“.

- **Core damage states**

As for the other anticipated transients, the core damage states in case of a "loss of main heat sink without loss of main feedwater" are characterized by high pressure in the primary circuit. In most cases (72 %) the core damage state occurs after 2 - 4 h (core damage state no. 10). For the remaining 28 %, induced by failures of the main steam release and failures of the accident management measure PBF, the time periods are below 2 h (core damage state no. 9). After occurrence of a core damage, the high pressure and the low pressure injections are available.

- **Contributions of system function failures**

In case of a "loss of main heat sink without loss of main feedwater" failures of the steam generator feedwater supply (leading to a system damage state) and of the accident management measures SBF and PBF play an essential role (73 %). In particular, failures to run of the demineralized water pumps, CCF of the main load control valves (failure to close), and CCF of the low-load control valves (failure to open) lead to a failure of the operational steam generator feedwater supply. The feedwater supply by the emergency feedwater system fails mainly due to CCF of the pressure level control valves (failure to open) and by CCF the emergency feedwater diesels (failure to start).

For the failure of SBF and PBF failures of the manual actions play the most important role.

- **Contributions of individual failure causes (importances)**

Failures of the manual actions for PBF (100 %) and SBF (42 %) have the highest importance for the core damage frequency. CCF of the main steam release isolation valves and of the safety valves (main valves) contribute 19 %. Further important failure causes are the CCF of the four pressure level control valves of the emergency feedwater system (17 %), failures to run of the demineralized water injection pumps (15 %), and the following CCF (4 of 4 each): emergency feedwater diesels fail to start (14 %), emergency feedwater isolation valves fail to open (14 %), main load control valves fail to close, and low-load control valves fail to open (13 % each).

CCF in total contribute 97 %, human failures contribute 100 % to the core damage frequency.

5.3.3.9 Loss of main feedwater and loss of main heat sink

- **Accident management measures to cope with the system damage states**

As with the anticipated transients treated before, in case of a system damage state induced by a loss of main heat sink and loss of main feedwater, core damage can be prevented by the accident management measures SBF resp. repair or PBF. The event sequences and the minimum requirements to the system functions (SBF, PBF) are the same as for the loss of preferred power (see section 5.3.3.6). The relevant time periods for performing the manual actions have been estimated based on thermal hydraulic calculations for the loss of main feedwater without loss of main heat sink.

- **Transition probabilities from system damage states to core damage states**

In case of a "loss of main heat sink and loss of main feedwater", the probability of transition from a system damage state to a core damage state is $3,8 \cdot 10^{-2}$. This means, that approx. 4 % of the system damage states lead to core damage. In most cases (96 %) the plant can be transferred into a safe state by the accident management measures

SBF resp. repair or PBF. The main contribution to the failure of SBF and PBF comes from the failure of manual actions for performing the measures.

With the frequency of a system damage state in case of a loss of main heat sink and loss of main feedwater of $2,9 \cdot 10^{-7}/a$ (see section 5.2.8) and the transition probability of $3,8 \cdot 10^{-2}$ the core damage frequency in case of loss of main heat sink and loss of main feedwater is $1 \cdot 10^{-8}/a$.

Similar to a "loss of main heat sink without loss of main feedwater" the result for the frequency of the system damage states is dominated by the system damage state no. 7 (94 %) with a failure of the steam generator feedwater supply. After failure of SBF resp. repair and PBF the system damage state leads to core damage state no. 10. The respective transition probability is $2,7 \cdot 10^{-2}$. In most cases (approx. 63 %) failure of SBF and PBF is caused by human failures. In the remaining cases (approx. 37 %), valve failures lead to failures of SBF. A failure of the repair measures considered in this PSA (see section 5.3.1.2) is caused either by a too short time period or by human failures (see section 5.3.3.7). Nearly 10 % of the frequency of core damage state no. 10 are correlated to failure combinations including the non-closure of a main steam safety valve (failure to close after opening). The respective statements in section 5.3.3.8 are valid also in this case.

As for the other anticipated transients, the transition probability from the system damage state no. 6 (failure of the main steam pressure limitation) to the core damage state no. 9 is 0.18 (see sections 5.3.3.6 to 5.3.3.8).

- **Transition probabilities from the initiating event to core damage states**

The probability of transition from the initiating event to a core damage state is $1,5 \cdot 10^{-6}$, with a contribution of 76 % from failures of the steam generator feedwater supply and the accident management measures SBF and PBF. Although, due to the initiating event, the main feedwater pumps cannot be used for the steam generator feedwater supply, the contribution is only slightly higher than in case of a "loss of main heat sink without loss of main feedwater" (73 %) because on the one side failures of the full-load control valves (failure to close) do not play a role for the failure of the operational feedwater supply and – on the other side - failures of the main steam pressure limitation and the failure of PBF with 24 % significantly contribute to the core damage frequency.

- **Core damage states**

As for the other anticipated transients the core damage states in case of a "loss of main heat sink and loss of main feedwater" are characterized by high pressure in the primary circuit. In most cases (70 %), the core damage state occurs after 2 - 4 h (core damage state no. 10). For the remaining 30 %, resulting from failures of the main steam release and failures of the accident management measure PBF, the time periods are below 2 h (core damage state no. 9). After occurrence of core damage the high pressure and the low pressure injection are available.

- **Contributions of system function failures**

In case of a "loss of main heat sink and loss of main feedwater" failures of the steam generator feedwater supply (leading to a system damage state) and of the accident management measures SBF and PBF play an essential role (76 %). In particular, the failure to run of the demineralized water injection pumps and the CCF of the low-load control valves (failure not open) lead to a failure of the operational steam generator feedwater supply. The injections by the emergency feedwater system fail mainly due to CCF of the pressure level control valves (failure to open) and by CCF of the emergency feedwater diesels (failure to start). For the failure of SBF and PBF human failures play the dominant role.

- **Contributions of individual failure causes (importances)**

Similar to the other anticipated transients except the loss of preferred power, failures of the manual actions for PBF (100 %) and SBF (42 %) have the highest importance for the core damage frequency. The CCF of the main steam release isolation valves and safety valves (main valves) contributes 20 %. Further important failure causes are the failure to run of the demineralized water pumps (17 %) and the following CCFs (4 of 4 each): emergency feedwater diesels do not start (15 %), low-load control valves do not open, pressurizer control valves of the emergency feedwater system do not open (14 % each), and emergency feedwater isolation valves do not open(13 %).

CCFs in total contribute 95 %, human failures contribute 100 % to the core damage frequency.

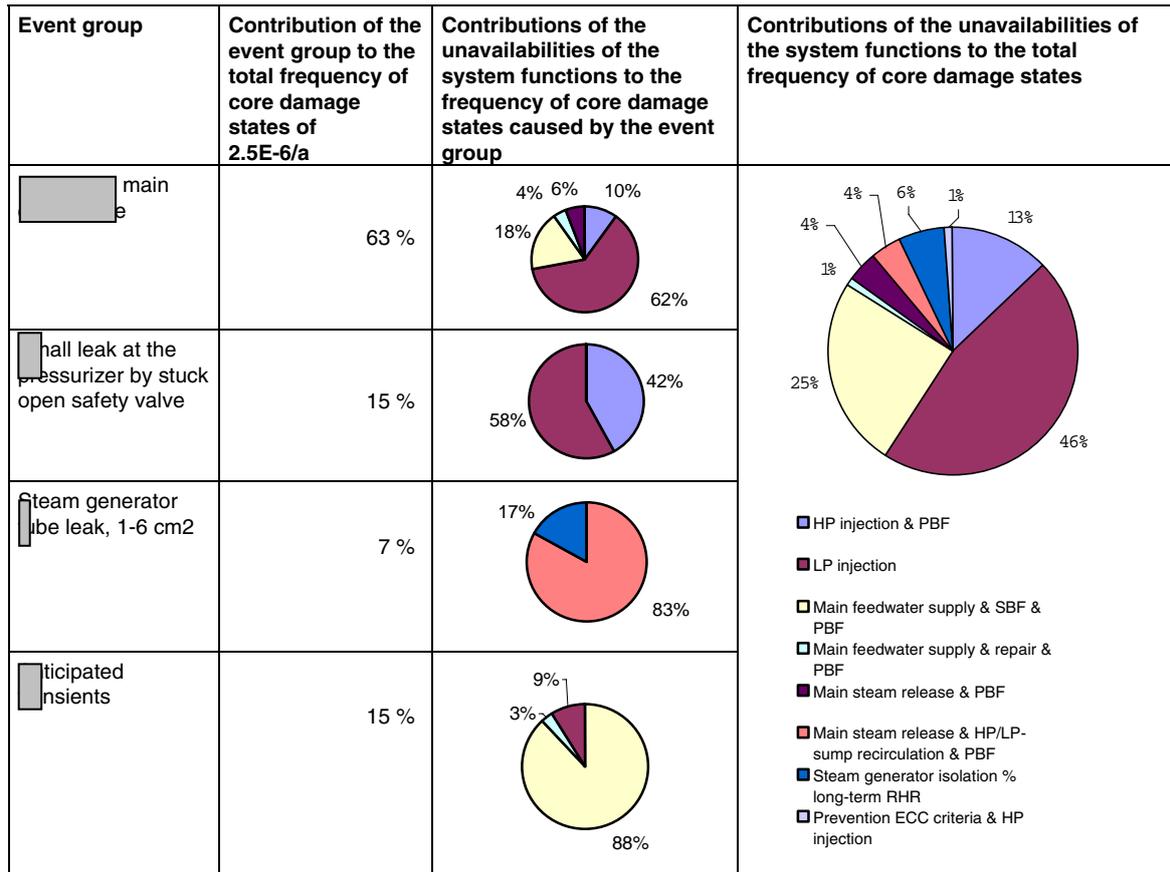
5.3.4 Summary of the results for core damage states

The total frequency of core damage states caused by plant internal initiating events is $2.5 \cdot 10^{-6}/a$. The frequency distribution calculated by the uncertainty analysis is described in section 5.4.

In the following, the transition probability from a system damage to a core damage state, characteristic attributes of the most frequent core damage states, and the contributions of the initiating events, of the system function failures and of individual failure causes are described (see tables 5.9 and 5.10 and figure 5.2).

- **Transition probability from a system damage to a core damage state**

The average probability (weighted by the frequency of system damage states) of the transition from a system damage state to a core damage state is 0.29. In case of LOCAs all system damage states lead to a core damage state. For an essential part of the sequences, the cause of the system damage state is a failure of the low pressure injections of the RHR system. In these cases, PBF cannot prevent a core damage state. In case of LOCAs, furthermore, the time period between actuation of the criteria for the preparation of the accident management measure PBF and the point of time, at which PBF must be effective to prevent a core damage state, is so short that PBF for the prevention of core damage state is hardly possible. In contrast, for anticipated transients transition probabilities between 0.2 ("loss of preferred power") and $2.5 \cdot 10^{-2}$ ("loss of main feedwater") are reached. The essential contributions to the unavailability of the accident management measures result from failures of the manual actions for performing the accident management measures SBF and PBF. The failure of the repair measures is of minor importance for the core damage states. The relatively high transition probability in case of a loss of preferred power is caused by system damage states due to a CCF of the 48 V batteries.



SG steam generator
 HP high pressure
 LP low pressure
 ECC emergency cooling criteria
 RHR residual heat removal
 PBF primary pressure feed and bleed
 SBF secondary pressure feed and bleed

Fig. 5.2 Contributions of the event groups of initiating events to the total core damage frequencies and contributions of unavailabilities of system functions

• **Core damage states**

The types of core damage states, which occur if design-basis system functions and the plant internal accident management and repair measures fail after an initiating event, are described in tables 5.9 and 5.11. These tables also depict the respective frequencies and the transition probabilities from an initiating event (table 5.11) resp. from a system damage state (table 5.9) to a core damage state. In three further tables the characteristic attributes

- Pressure in the primary circuit (table 5.13),

5.3 Transition from system damage states to core damage states

- availability of the primary-side injection after onset of a core damage (table 5.14) ,
and
- time period from the initiating event until onset of core damage (table 5.15)

are outlined in more detail. In these tables the transition probabilities from the initiating events to core damage states with the selected attributes are given. Small leaks at a main coolant line with leak cross sections $> 25 \text{ cm}^2$ are combined in the tables, because their contributions to the core damage frequencies are low and they are not much different from each other. Also the anticipated transients, except the loss of preferred power, are combined. The meaning of the terms in the tables is the following:

- L < 25: small leak at a main coolant line, 2 - 25 cm^2
(initiating event no. 4 in table 5.6)
- L > 25: leaks at a main coolant line, 25 - 200 cm^2
(initiating events 2 and 3 in table 5.6)
- LPR: leak at the pressurizer by stuck open safety valve
(initiating event 6 in table 5.6)
- SGL: steam generator tube leak, 1 - 6 cm^2
(initiating event 8 in table 5.6)
- LOP: loss of preferred power (initiating event 10 in table 5.6)
- T: anticipated transients, except loss of preferred power
(initiating events 11 to 13 in table 5.6)

The frequencies of the individual initiating events can be found in table 5.1. For the combined initiating events the following frequencies have been calculated:

- L > 25: $2.4 \cdot 10^{-4}/\text{a}$
- T: $1.7 \cdot 10^{-1}/\text{a}$

The total frequency of all initiating events is $2.0 \cdot 10^{-1}/\text{a}$ (column "all" in sections 5.13 to 5.15).

- **Contributions of the initiating events**

The highest contributions to the core damage frequency result from

- a small leak at a main coolant line, 2 - 25 cm² (53 %),
- a leak at the pressurizer by stuck open safety valve (15 %), and from
- a loss of preferred power (10 %).

Other leaks at a main coolant line (25 - 200 cm²) together contribute 10 %, the steam generator tube leak, 1 - 6 cm², contributes 7 %, and the other anticipated transients 5 %.

LOCAs by leaks in a primary coolant line inside the containment or by a pressurizer leak together have a dominating contribution of nearly 80 %. Anticipated transients and the steam generator tube leak are of minor importance. For the frequency of system damage states the order is inverted: The major contribution of 70 % results from anticipated transients, LOCA bring only a contribution of 22 % (see section 5.2.12). This shows that plant internal accident management and repair measures in case of anticipated transients essentially contribute to the prevention of core damage states. In case of LOCAs, we assumed – based on the criteria defined in the emergency manual for the initiation of accident management measures -, that the available time periods are too short to perform the measures successfully.

The contributions of the individual initiating events to the core damage frequency can be seen from table 5.12. The probabilities of the transition from initiating events to core damage states together with selected attributes are outlined in tables 5.13 to 5.15.

- **Contributions of system function failures to the transition from a system damage to a core damage state**

The main contributions to the probabilities for transition from a system damage state to a core damage state are listed in table 5.10 for the initiating events (the transition probabilities are equivalent to the unavailabilities of plant internal accident management and repair measures). The table also shows the causes for the failure of accident management and repair measures, differentiating between the following causes (see section 5.3.3):

- System failures (column "SF")

- the time period between reaching the criteria for the preparation of accident management measures and the point of time, at which these measures must be effective, is not sufficient to perform successfully the measure for preventing a core damage (column "C")
- failure of the manual actions in those cases, for which the accident management measures can be performed due to the available system functions related and the temporal conditions (column "HF")

The probability of transition from a system damage to a core damage state includes the following contributions:

In approx. 50 % of the cases, accident management measures - due to the initiation resp. performing criteria defined in the emergency manual - are assessed not to be successful. This applies essentially to all system damage states from small leaks with failures of the high pressure injections or of the secondary-side system functions, the steam generator tube leak and the loss of preferred power with failure of all 48 V batteries.

In 44 % of all cases, PBF cannot be performed due to unfavorable system states. These are cases with a small leak at a main coolant line resp. a leak at the pressurizer with failure of the low pressure injections.

The remaining contribution of approx. 6 % results from the failure of SBF and PBF in case of anticipated transients.

- **Contributions of system function failures to the transition from initiating events to a core damage state**

The probabilities of transition from an initiating event to a core damage state are shown in table 5.12 (see also figure 5.2). The failure of the low pressure injections in case of small leaks contribute 46 % to the total transition probability. In these cases, PBF fails because of system function failures. Mainly independent failures of the water level measurements of the cell coolers in the residual heat removal system contribute to the failure of the low pressure injections. 25 % of the core damage frequency result from failures of the steam generator feedwater supply with failure of the accident management measures SBF and PBF, whereby small leaks and anticipated transients contribute to equal parts. In case of small leaks, the success probability of accident manage-

ment measures is assessed to be low because of the existing criteria for preparing and performing these measures. In case of transients, the loss of preferred power with a simultaneous battery CCF plays an essential role. In our opinion, this situation is not sufficiently covered by the emergency manual. Besides the CCF mentioned above (in case of loss of preferred power), CCFs of valves in the injection lines and failures to run of the emergency feedwater and demineralized water pumps are the dominating causes of the failure of the steam generator feedwater supply. 24 % result essentially from failures of the high pressure injections or of the feedwater supply in case of small leaks. PBF is assessed not to be successful for these sequences due to the criteria defined for preparing resp. performing accident management measures. For 14 %, first of all the feedwater supply fails in case of anticipated transients. SBF and PBF are failed in case of these sequences, because a situation prevails, which in our opinion is not sufficiently covered by the emergency manual (loss of preferred power with CCF of all 48 V batteries, 8 %) or due to human failures (6 %).

Table 5.16, analogous to tables 5.13 to 5.15, presents the probabilities of transition from initiating events to core damage states with the responsible failed system functions.

5.3 Transition from system damage states to core damage states

Table 5 Probabilities of the transition from initiating events to core damage states

- .13 with high, medium, low pressure
- .14 with availability of primary injection systems
- .15 for selected time periods

Pressure in the primary circuit at the core damage state	Transition probability of initiating events ¹⁾ (x E-3) (Designation) ²⁾						
	L<25	L>25	LPR	SG TL	LPP	T	all
high pressure (> 10 MPa)	0.091				0.01	0.001	0.003
medium pressure (1 – 10 MPa)	0.05	0.728	0.2	0.086			0.003
low pressure (< 1 MPa)	0.296	0.316	0.28				0.006
Availability of primary-side injection at the core damage state							
neither HP nor LP systems available	0.296	0.316	0.28	0.072	0.009		0.008
Only LP systems available	0.05	0.728	0.2	0.014			0.003
HP systems in the long-term or HP and LP systems available	0.091				0.001	0.001	0.002
Time period from initiating event until core damage state							
Less than 2 hours	0.098	0.343	0.2				0.003
2 to 4 hours		0.638	0.28	0.014	0.01	0.001	0.004
4 to 12 hours	0.326			0.072			0.006
more than 12 hours	0.014	0.063					

1) frequencies see table 5.1 and page 159
 2) see page 159
 HP high pressure
 SGT steam generator tube leak

LPR pressurizer leak
 LP low pressure
 T transients
 LPP loss of preferred power

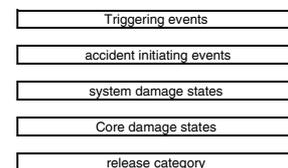


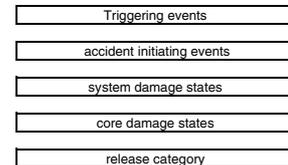
Table 5.16 Probabilities of transition from initiating events to core damage states due system function failures

Failed system functions at core damage state	Transition probability of initiating events ¹⁾ (x E-3) (Designation)							
	L<25	L>25	PL	SGTL	LOP	T	all	
HP injection and PBF	0.007	0.645	0.2					0.002
LP injection	0.296	0.316	0.28					0.006
SG injection and SBF an PBF	0.092	0.055			0.009	0.001		0.003
SG injection and repair und PBF								
100K/h-shutdown and HP sump recirculation and PBF	0.031	0.028						
shutdown and PBF	0.009							
FD pressure control/limitation and PBF					0.001			
SG isolation and long-term RHR (SG tube leak)				0.072				0.001
prevention of emergency cooling criteria and HP injection (SG tube leak)				0.014				

1) frequencies see table 5.1

SG steam generator
MS main steam
HP high pressure
LP low pressure
SGTL SG tube leak
PL prssuriser leak

PBF primary pressure feed and bleed
SBF secondary pressure feed and bleed
T transients
LOP loss of preferred power



• **Contributions of individual failure causes (importances)**

With a contribution of approx. 25 % independent failures of the water level measurements of the cell coolers of the residual heat removal system play an essential role. CCFs of the main steam relief control valves and of the 48 V-batteries of the D2-grid each contribute nearly 10 % to the frequency of core damage states. The manual actions for performing accident management measures are of minor importance with contributions of 6 % (PBF) and 3 % (SBF). In most cases, accident management measures are assessed not to be successful because of the defined criteria for preparing and performing accident management measures. Also the failure of repair measures in case of anticipated transients does not significantly influence the result. The cause is that a sufficiently long time period must be in order to successfully perform the repair

measures. For this purpose, the accident management measure SBF to use the water inventory of the feedwater lines and of the feedwater tank has to be performed. It is assumed, that even simple repair measures cannot be performed successfully if this accident management measure fails.

CCFs in total contribute 73 % to the core damage frequency, human failures in total contribute 14 %.

The results can be summarized in a very generalized manner as follows:

- Transients lead nearly exclusively to early core damage states under high pressure. The primary-side injection is available, if the transient has not been caused by a loss of preferred power.
- Small leaks are the most frequent initiating events leading to core damage states. The pressure is – as for medium leaks – in most cases low. For event sequences, which lead to core damages, in most cases injection systems are not available.
- Steam generator tube leaks lead to a core damage state only after a longer time period. The pressure is at a medium level, injection systems are in most cases not available for those sequences which lead to core damage.

5.4 Uncertainties of the results of the reliability analysis

The frequencies of the initiating events and the reliability data for the system components and for manual actions are not exactly known. The knowledge uncertainty ("epistemic uncertainty") of these data is expressed by subjective probability distributions. It was common practice up to now to calculate point values for the frequencies of system and core damage states and for the unavailabilities of the system functions using - as input data - the mean values of the probability distributions for the frequencies of triggering resp. initiating events and for the component reliability data. Based on the insights from the present PSA, it is no longer deemed appropriate to apply point values as representative results of the PSA. As representative results mean values in connection with the quantified uncertainties should be used. Point values are therefore listed in the present PSA, only if this is sensible for assessing the applied PSA methods.

In the present PSA, for all important results (frequencies, unavailabilities, importances, see tables 5.5 to 5.16) the mean values of their resulting subjective probability distribu-

tions have been calculated by means of uncertainty analyses. These analyses have been performed for each individual system damage resp. core damage state (approx. 40 sequences each) by means of Monte Carlo simulations with a sample size of 5000. This sample size is sufficient to get standard deviations for the estimated mean values for the relevant sequences, which are not larger than approx. 10 % of the respective mean. This criterion is appropriate to define the required number of simulation runs. The results for groups of system damage resp. core damage states (e.g. frequency of all system damage states caused by a specific initiating event) have been calculated by summing up all mean values of the frequencies of individual sequences.

The uncertainty analyses have been performed based on the minimum cuts identified by means of point value calculations. "Minimum cuts" are those combinations of component failures, which are exactly sufficient to cause a failure of the analyzed system function. The minimum cuts have been calculated with the PSA program "Risk Spectrum PSA Professional" (Version 1.10.02). Due to calculational reasons, the number of minimum cuts used as basis for the uncertainty analysis was limited to 50000 per event sequence. It has been estimated, that the neglected minimum cuts would influence the result only insignificantly.

It has to be stated, that the PSA results are connected with further uncertainties, which have not been quantified in this study (e.g. model uncertainties) or which cannot be quantified in general (e.g. the uncertainty, whether unknown but potentially relevant phenomena have been neglected).

- **State-of-knowledge dependency ("failure rate coupling")**

The subjective probability distributions and their fractiles and mean values have been calculated by means of a simulative method /GRS 90/ taking into account the state-of-knowledge dependencies of the component reliability data and the data for the reliability of manual actions ("failure rate coupling"). State-of-knowledge dependency has been assumed for the reliability data of those components, for which the operating experience has been pooled for the evaluation of the reliability data. Specifically, the approach was as follows:

For the data for independent failures of process engineering and electric/electronic components the state-of-knowledge dependency due to the basic information sources has been taken into account. The same is valid for the CCF data. For independent fail-

ures of components of the I&C-system, all data - in a simplified approach - have been treated as state-of-knowledge dependent. This pessimistic approach has been chosen, because the respective I&C data partly include failure rates resp. failure probabilities of the same electronic circuits. To differentiate contributions with respect to their different data bases would have been very time consuming. This effort did not seem to be justified, because the chosen approach does not significantly affect the results of the uncertainty analysis. The approach was similar for the failure probabilities of manual actions, which in part including contributions from identical tasks.

- **Mean values vs. point estimates**

The mean values of the unavailabilities for the combinations of component functions, which contain basic events with “coupled” reliability data, are principally higher than the point values of these unavailabilities (calculated from the mean values of the reliability data). The deviations are increasing with increasing number of “coupled” basic events in a failure combination. The deviation also depends on the uncertainties of the “coupled” reliability data. The deviations between the point values and the mean values increase with the uncertainty of the reliability data of the “coupled” basic events included in the failure combination. The deviations for the frequencies of system damage resp. core damage states depend on the contribution to the total result from failure combinations with significantly different point values and mean values. According to the deviations of the frequencies of system damage resp. core damage states, the uncertainty analysis provides differing values also for the mean values of the importances of component failures and failure modes compared to the point value calculations. As far as we know, mean values for the importances (based on the subjective probability distributions of the reliability data) cannot be calculated by the commonly applied PSA computer codes. GRS therefore has improved the GRS code STREUSL.

- **Subjective probability distributions of the reliability data**

In the PSA, the uncertainties of the failure rates resp. failure probabilities often are characterized by adapted logarithmic normal distributions (abbr.: lognormal-distribution). The lognormal-distributions are adapted to the (empirical) subjective probability distributions of the reliability data applying the Bayesian approach by keeping fixed the 95% and 50% fractiles of these distributions to the corresponding fractiles of the lognormal-distributions /FAK 97a/. This approach has first been chosen also for

this PSA. However, in our opinion, the PSA should in general use Gamma distributions for failure rates and Beta distributions for failure probabilities. The application of log-normal-distributions for failure probabilities can cause significant distortions of the mean values and of the distributions of the unavailabilities of system functions resp. of the frequencies of system damage and core damage states. This is particularly valid if failure combinations with coupled failure probabilities are relevant for the results. In this PSA, therefore, Beta distributions have been applied for selected failure probabilities. A complete “change“ for the failure probabilities data base from lognormal- to Beta-distributions was not possible in this PSA due to restrictions of time and effort. In our view, there is a need for further investigation and testing of the methods and their application in a PSA. The selection of the basic events with failure probabilities, for which the Beta distributions have been adapted, were oriented on the mean values (orientation value: $> 1 \cdot 10^{-3}$), concerning mainly the failure probabilities of manual actions.

The state-of-knowledge uncertainties on the reliability data applied in the PSA, are expressed by the following distributions:

- Gamma distributions for the frequencies of anticipated transients
- Lognormal distributions for
 - the frequencies of other initiating events
 - failure rates for components
 - failure probabilities for components (in general)
- Beta distributions for
 - probabilities of human failures (adapted Beta distributions)
 - failure probabilities for components (for selected basic events)

The Beta distributions have been adapted to the 50% and 95% fractiles of the log-normal-distributions calculated in the assessment procedures (for manual actions THERP and ASEP).

The results of the uncertainty analysis for the frequencies of system damage and core damage states are described in the following sections and listed in tables 5.17 to 5.20. In part, point estimates are given for comparison. Figures 5.3 and 5.6 depict the subjective probability distributions of the total frequencies of system damage resp. core damage states resulting from plant internal initiating events.

5.4.1 Results of the uncertainty analysis for system damage states

- **System damage states sorted by the individual initiating events**

The results of the uncertainty analysis for the frequencies (1/a) of system damage states, differentiated by the initiating events, are displayed in table 5.17. As a measure for the uncertainty of the frequency the relation between the 95% fractile and the 5% fractile can be taken. The uncertainties of the frequencies of the initiating events and the uncertainties of the transition probabilities from an initiating event to a system damage state (unavailabilities of the system functions) contribute to the uncertainty of the results. The 5% , 50%, and 95% fractiles and the mean values of the subjective probability distributions of the frequencies of the initiating events are listed in table 5.18. Table 5.19 contains the respective fractiles of the subjective probability distributions and the corresponding mean values of the transition probabilities. Point values are given for comparison.

As can be derived from the fractiles given in table 5.17, significant differences exist between the uncertainties of the frequencies of system damage states for individual initiating events. So, the quotient between the 95% and the 5% fractiles in case of a “loss of preferred power“ is 6 (lowest value) and in case of a “loss of main feedwater and loss of main heat sink“ is 17 (highest value). If not only the 95% and 50% fractiles are compared, but also the lower fractiles of the distributions, the following result can be derived for the example of these initiating events: the quotient of the 50% fractiles and the 5% fractiles deviates stronger from each other in both cases (factor of 4 in case of a “loss of preferred power“ resp. a factor of 135 in case of a “loss of main feedwater and loss of main heat sink“) than the relation of the 95% and the 50% fractiles (factor of 6 resp. 17). For the “loss of main feedwater and loss of main heat sink“ the 5%-fractile of the frequency is relatively low (approx. $5 \cdot 10^{-10}$). The cause for the very broad distribution is the uncertainty of the frequency of the initiating event “loss of main feedwater and loss of main heat sink“. During the observation period, a “loss of main feedwater and loss of main heat sink“ did not occur (zero failure statistics). If no failure did occur, a relation of 940 between the 95% and the 5% fractiles results for the subjective probability distribution of the Gamma type. For the „loss of preferred power“ this value is “only” 3.6, because a relatively large number of such events has been observed (see table 5.18).

Also the uncertainty of the unavailability of system functions to cope with the initiating event (transition probabilities) contributes to the uncertainty of the frequency of a system damage state, caused by a specific initiating event. In this respect, however, the difference between a “loss of preferred power“ and a “loss of main feedwater and loss of main heat sink“ is much lower than for the frequency of the initiating event: The relation between the 95% fractile and the 5% fractile is 15 resp. 20 (see table 5.19). The slightly higher uncertainty for the “loss of main feedwater and loss of main heat sink“ can be attributed to the higher contribution from failure combinations with coupled failure rates resp. failure probabilities.

The uncertainties of the frequencies for system damage states induced by the anticipated transients „loss of main feedwater without loss of main heat sink“ and “loss of main heat sink without loss of main feedwater“, with a relation between 95% fractiles and 5% fractile of 8 resp. 10, are higher than for a “loss of preferred power“. In both cases, the transition probabilities contribute to these higher uncertainties. For the “loss of main heat sink without loss of main feedwater“ additionally the higher uncertainty of the frequency of the initiating event plays a role.

For the other initiating events, with the exception of the “small leak at a main coolant line, 2 - 25 cm²“ the relative values are between about 13 and 16.

As shown in table 5.17, the mean values of the frequencies are by a factor of up to approx. 2.4 (“loss of main heat sink without loss of main feedwater“) higher than the respective point values. This difference results from those failure combinations, which contain the failures of more than one component with coupled failure rates.

- **Total frequency of the event "system damage state"**

The results of the uncertainty analysis for the total frequency of the event "system damage state" are shown in the bottom line of table 5.17 and in figure 5.3. The factor between the 95% and the 5% fractile is approx. 4.4. The quantified uncertainty is in a range, which is not unusual for the investigation of very improbable events. As already mentioned, the results of the PSA are inflicted with further uncertainties which have not been quantified in this analysis (e.g. model uncertainties) or which cannot be quantified in principle.

The mean value of the system damage frequency with $8,2 \cdot 10^{-6}$ is higher than the respective point estimate by a factor of approx. 1.7.

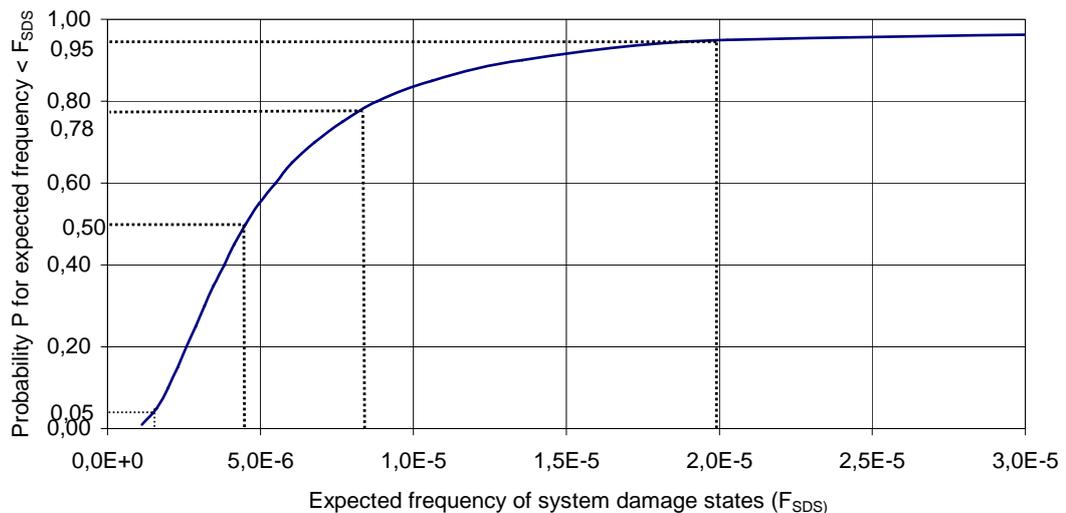


Fig. 5.3 Subjective probability distribution of the frequency of the event "system damage state" (only plant internal initiating events)

Table 5.17 Fractiles, point values and mean values of the frequencies of system damage states sorted by initiating events

1) No.	Initiating event Name/Type	Uncertainties of the results concerning system damage state frequencies (1/a)				
		5% fractile	50% fractile	Point value	Mean value	95% fractile
2	small leak, 80 - 200 cm ²	1.2E-9	1.6E-8	4.2E-8	9.1E-8	2.6E-7
3	small leak, 25 - 80 cm ²	2.4E-9	3.4E-8	7.8E-8	1.5E-7	5.2E-7
4	small leak, 2 - 25 cm ²	1.3E-7	6.3E-7	8.4E-7	1.3E-6	4.2E-6
6	small pressurizer leak	8.1E-9	1.0E-7	2.6E-7	3.7E-7	1.4E-6
8	small SG tube leak	3.6E-9	5.1E-8	1.8E-7	1.8E-7	7.6E-7
10	loss of preferred power	1.8E-7	7.4E-7	9.6E-7	1.5E-6	4.2E-6
11	loss of MFW without loss of MHS	1.7E-7	8.3E-7	1.3E-6	2.2E-6	6.3E-6
12	loss of MHS with- out loss of MFW	8.2E-8	5.6E-7	7.8E-7	1.9E-6	5.3E-6
13	loss of MFW and of MHS	4.9E-10	6.6E-8	1.6E-7	3.7E-7	1.1E-6
15	MS line break out- side containment	2.3E-9	3.4E-8	1.2E-7	1.3E-7	5.3E-7
17	MFW line break outside contain- ment	6.6E-9	7.5E-8	2.2E-7	2.7E-7	1.0E-6
	Total values	1.6E-6	4.5E6	4.8E-6	8.2E-6	2.0E-5

1) see table 5.1
SG steam generator
MS main steam

MFW main feedwater
MHS main heat sink
FW feedwater

Table 5.18 Fractiles and mean values of the frequencies of initiating events

Initiating event		Frequencies (1/a)			
No ¹⁾	Designation	5% fractile	50% fractile	Mean value	95% fractile
2	small leak, 80 - 200 cm ²	3.4E-6	3.4E-5	9.0E-5	3.4E-4
3	small leak, 25 - 80 cm ²	5.5E-6	5.8E-5	1.5E-4	5.1E-4
4	small leak, 2 - 25 cm ²	7.6E-4	2.3E-3	3.0E-3	7.5E-3
6	small pressurizer leak	3.2E-5	3.2E-4	8.5E-5	3.2E-3
8	small SG tube leak	1.2E-4	1.0E-3	2.3E-3	8.0E-3
10	loss of preferred power	1.2E-2	2.4E-2	2.5E-2	4.4E-2
11	loss of MFW without loss of MHS	5.5E-2	1.1E-1	1.2E-1	1.9E-1
12	loss of MHS without loss of MFW	8.5E-3	3.3E-2	3.8E-2	8.4E-2
13	loss of MFW and loss of MHS	3.0E-5	3.5E-3	7.5E-3	2.8E-2
15	MS line break outside containment	5.9E-6	6.0E-5	1.6E-4	5.9E-4
17	FW line break outside containment	1.0E-5	9.9E-5	2.6E-4	9.5E-4

1) see table 5.1
 SG steam generator
 MS main steam

MFW main feedwater
 MHS main heat sink
 FW feedwater

Table 5.19 Fractiles, point estimates and mean values of the transition probabilities from initiating event to system damage state

Initiating event		Probabilities				
No ¹	Designation	5% fractile	50% fractile	Point value	Mean value	95% fractile
2	small leak, 80 – 200 cm ²	1.7E-4	4.3E-4	4.6E-4	9.0E-4	2.3E-3
3	small leak, 25 – 80 cm ²	2.0E-4	4.8E-4	5.0E-4	9.6E-4	2.4E-3
4	small leak, 2 – 25 cm ²	9.4E-5	2.5E-4	2.7E-4	4.0E-4	1.1E-3
6	small pressurizer leak	1.2E-4	2.8E-4	3.0E-4	4.9E-4	1.1E-3
8	small SG tube leak	7.8E-6	4.5E-5	7.4E-5	8.6E-5	2.7E-4
10	loss of preferred power	8.8E-6	2.9E-5	3.6E-5	4.8E-5	1.3E-4
11	loss of MFW without loss of MHS	1.8E-6	7.73E-6	1.1E-5	1.7E-5	5.0E-5
12	loss of MHS without loss of MFW	4.2E-6	1.7E-5	2.1E-5	3.7E-5	1.1E-4
13	loss of MFW and loss of MHS	5.0E-6	1.8E-5	2.2E-5	3.4E-5	9.9E-5
15	MS line break outside containment	1.5E-4	5.5E-4	7.8E-4	8.4E-4	2.4E-3
17	FW line break outside containment	3.0E-4	7.4E-4	8.3E-4	1.2E-3	2.5E-3

1) see table 5.1
 SG steam generator
 MS main steam

MFW main feedwater
 MHS heat sink
 FW feedwater

5.4.2 Results of the uncertainty analysis for core damage states

- **Core damage states sorted by initiating events**

The results of the uncertainty analyses for core damage states are shown in tables 5.20 and 5.21 and in figure 5.4. Table 5.20 and figure 5.4 show the fractiles and the mean values of the distributions and, for comparison, the point values of the core damage frequencies for the individual initiating events (only table 5.20). In table 5.21, the fractiles and the mean values of the subjective probability distributions and the point values for the probabilities of the transition from an initiating event to a core damage state are listed.

The uncertainties of the core damage frequencies (1/a) for the LOCAs are the same as those for the system damage frequencies (see table 5.17), because for these initiating events accident management and repair measures have not been considered (see section 5.3). For the anticipated transients the uncertainties are higher due to the uncertainties of the failure probabilities of the considered accident management and repair measures. Related to the quotients of the 95% and 5% fractiles of the subjective probability distributions of the system damage state frequencies for these transients the subjective probability distributions of the core damage states are broader by a factor of approx. 2 (“loss of preferred power”) up to approx. 18 (“loss of main heat sink without loss of main feedwater”). The relatively small increase of the uncertainty for the “loss of preferred power” results from the fact that for an essential part of the sequences accident management and repair measures have not been considered (e.g. if a CCF of all four 48 V batteries of the emergency power system 2 occurs, see section 5.3.3.6). Therefore, failures of the accident management and repair measures are of minor importance. For the other anticipated transients, mainly the uncertainties of the failure probabilities for personnel actions in case of accident management and repair measures contribute to the increase in the uncertainties.

Similar to the system damage frequencies, the mean values are in maximum by a factor of approx. 2 higher than the point values. This increase results from those failure combinations which contain a failure of several components resp. several human actions with coupled reliability data.

- **Combined core damage states**

The results of the uncertainty analyses for the frequencies of the combined core damage states (see section 5.3.2) are displayed in table 5.22 and in figure 5.5. The factor between the 5% and the 95% fractiles varies from 31 (core damage state no. 3) to approx. 750 (core damage state 10). Core damage state no. 3 results essentially from a “small leak at a main coolant line, 2 – 25 cm²” with a relatively low uncertainty of the occurrence frequency (see table 5.18). Furthermore, accident management and repair measures have not been considered for this initiating event, in contrast to the anticipated transients (see section 5.3), so that uncertainties of the failure probabilities of these measures do not influence the result. Core damage state no. 10, in contrast, is caused by uncontrolled anticipated transients with failure of SBF resp. repair and PBF. In this case, in part much higher uncertainties for the probabilities for the transition from the initiating event to a core damage state contribute to the result (see table 5.21).

- **Total frequency of the event “core damage state“**

The results of the uncertainty analysis for the total frequency of the event “core damage state“ are shown in the bottom line of tables 5.20 and 5.22 and in figures 5.4 to 5.6. The mean value of the frequency is $2.5 \cdot 10^{-6}$, the 95% fractile is $7.3 \cdot 10^{-6}$ and the 5% fractile is approx. $4.4 \cdot 10^{-7}$. The quotient between the 95% and the 5% fractile is approx. 17 and thus slightly higher than for the total frequency of the event “system damage state“ (13, see table 5.17). The increase results from those anticipated transients, for which the uncertainties of the failures of human actions for the accident management resp. repair measures play a role. The increase is relatively slight, because the anticipated transients are only minor significant for the total result (15 %, see section 5.3.4).

The mean value of $2.5 \cdot 10^{-6}/a$ is by a factor of approx. 1.5 higher than the respective point value ($1.7 \cdot 10^{-6}/a$). The difference between mean value and point value is a bit lower than for the frequency of system damage states (mean value / point value = 2). It is nearly equal to the values for LOCAs, which bring the major contribution to the core damage frequency (see section 5.3.4).

Table 5.20 Fractiles, point estimates and mean values of the core damage frequency sorted by initiating events

Initiating event		Frequencies (1/a)				
No.	Designation	5% fractile	50% fractile	Point value	Mean value	95% fractile
2	small leak, 80 - 200 cm ²	1.2E-9	1.6E-8	4.2E-8	9.1E-8	2.6E-7
3	small leak, 25 - 80 cm ²	2.4E-9	3.4E-8	7.8E-8	1.5E-7	5.2E-7
4	small leak, 2 - 25 cm ²	1.3E-7	6.3E-7	8.4E-7	1.3E-6	4.2E-6
6	small pressurizer leak	8.1E-9	1.0E-7	2.6E-7	3.7E-7	1.4E-6
8	small SG tube leak	3.6E-9	5.1E-8	1.8E-7	1.8E-7	7.6E-7
10	loss of preferred power	1.1E-8	9.3E-8	2.2E-7	2.5E-7	9.4E-7
11	loss of MFW without loss of MHS	2.0E-10	8.5E-9	2.6E-8	5.5E-8	2.2E-7
12	loss of MHS without loss of MFW	2.0E-10	1.0E-8	3.0E-8	6.0E-8	2.3E-7
13	loss of MFW and of MHS	3.0E-12	9.0E-10	6.0E-9	1.1E-8	4.5E-8
Total values		4.4E-7	1.5E-6	1.7E-6	2.5E-6	7.3E-6

1) see table 5.1
 SG steam generator
 MFW main feedwater
 MHS main heat sink

Table 5.21 Fractiles, point estimates and mean values of the transition probabilities from initiating events to core damage

Initiating event		Probabilities				
No. ¹⁾	Designation	5% fractile	50% fractile	Point value	Mean value	95% fractile
2	small leak, 80 - 200 cm ²	1.7E-4	4.3E-4	4.6E-4	9.0E-4	2.3E-3
3	small leak, 25 - 80 cm ²	2.0E-4	4.8E-4	5.0E-4	9.6E-4	2.4E-3
4	small leak, 2 - 25 cm ²	9.4E-5	2.5E-4	2.7E-4	4.0E-4	1.1E-3
6	small pressurizer leak	1.2E-4	2.8E-4	3.0E-4	4.9E-4	1.1E-3
8	small SG tube leak	7.8E-6	4.5E-5	7.4E-5	8.6E-5	2.7E-4
10	Loss of preferred power	5.0E-7	3.9E-6	9.0E-6	9.4E-6	3.2E-5
11	Loss of MFW without loss of MHS	2.5E-9	8.5E-8	2.2E-7	5.0E-7	1.8E-6
12	Loss of MHS without loss of MFW	1.0E-8	3.4E-7	8.0E-7	1.4E-6	5.1E-6
13	Loss of MFW and of MHS	9.8E-9	3.3E-7	7.9E-7	1.3E-6	5.1E-6

1) see table 5.1
SG steam generator

MFW main feedwater
MHS main heat sink

Table 5.22 Fractiles, point estimates and mean values of the frequencies of core damage states

No	Core damage state			Frequencies (1/a)				
	A	P	t [h]	5% fractile	50% fractile	Point value	Mean value	95% fractile
1)								
2	no HP, no LP	LP	2 - 4	1.5E-8	1.0E-7	2.1E-7	2.8E-7	1.0E-6
3	no HP, no LP	LP	4 - 12	9.0E-8	4.1E-7	6.0E-7	8.7E-7	2.8E-6
4	only LP	MP	< 2	1.2E-8	6.9E-8	1.4E-7	2.7E-7	7.7E-7
5	only LP	MP	2 - 4	2.5E-9	2.0E-8	4.0E-8	9.5E-8	2.9E-7
6	only LP	MP	4 - 12	1.5E-9	1.9E-8	4.4E-8	9.0E-8	3.1E-7
7	no HP, no LP	MP	4 - 12	2.3E-9	3.9E-8	1.6E-7	1.6E-7	6.1E-7
8	only LP	MP	> 12	1.3E-9	1.5E-8	3.9E-8	6.5E-8	2.2E-7
9	only HP or HP and LP	HP	< 2	1.0E-8	8.5E-8	1.8E-7	3.1E-7	1.0E-6
10	only HP or HP and LP	HP	2 - 4	6.6E-10	2.4E-8	6.0E-8	1.3E-7	5.1E-7
11	no HP, no LP	HP	2 - 4	4.8E-9	6.1E-8	2.0E-7	2.2E-7	8.3E-7
Total values				4.4E-7	1.5E-6	1.7E-6	2.5E-6	7.3E-6

1) see table 5.8

A availability of primary-side injection

P pressure in the reactor coolant system

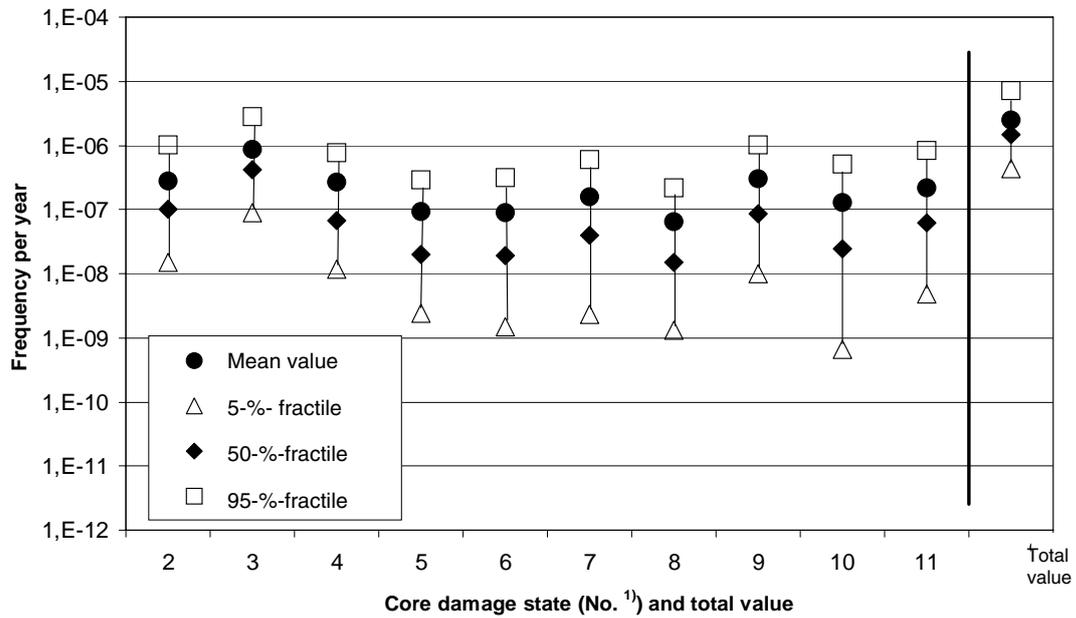
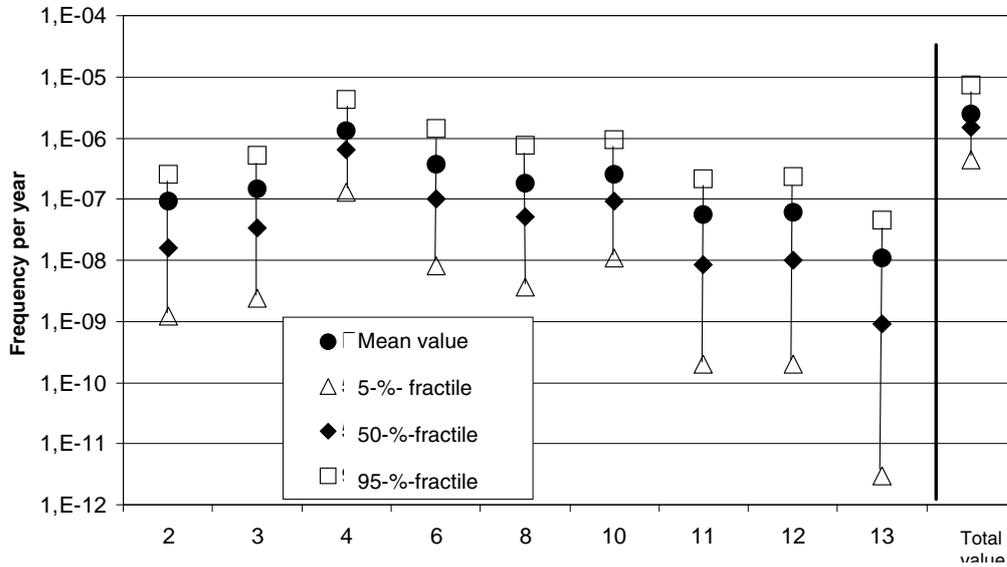
HP high pressure

MP medium pressure

LP low pressure

t time period until core damage

5 Level 1 PSA for power operation



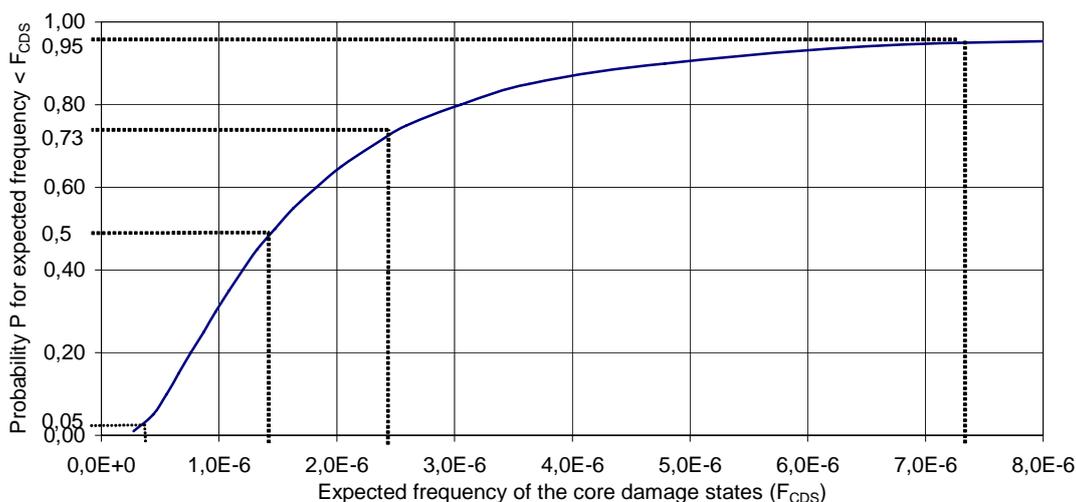


Fig. 5.6 Subjective probability distribution of the annual event frequency of the event "core damage state" (only plant internal initiating events)

5.5 Insights with respect to the PSA methods and to the plant design

5.5.1 PSA methods

With respect to the methods for a level 1 PSA for power operation, the present PSA has provided the following insights:

- Particularly for nuclear power plants with a very high safety level and accordingly very low frequencies of damage states, the results of the analyses are very sensitive to minor modifications in the assumptions and input data. Sensitivity analyses can help to identify and – if possible – to confirm the important parameters.
- Because the limitation of the effort for the analysis in principle requires an iterative approach, the degree of detail of the fault tree and event tree analyses should not be restricted too early based on quantitative (and qualitative) "cut off criteria".
- The core damage and plant damage frequencies (release frequencies) calculated by the analyses, should be used to check if it is justified to neglect certain initiating events resp. event sequences.

5 Level 1 PSA for power operation

- The original approach to modify the Basis-PSA with respect to dominating contributions turned out to be inefficient. By the modification of the modeling again and again other contributions became dominant, so that finally it would have been more efficient to modify the event tree and systems analyses in a comprehensive manner from the beginning.
- The (exemplary) consideration of repair measures, which required relatively high analytical effort, did hardly influence the result, because for the case analyzed in this PSA the time period available for repair is too short. Nevertheless, the methods to take into account repair measures should be improved, in order to allow a realistic modeling of the plant specific conditions.
- For an efficient treatment of the interface between level 1 and level 2 of the PSA, a specific program for evaluation of the event trees and fault trees should be developed.
- For a detailed analysis of the event sequences including the available time periods for personnel actions, the application of plant simulators is recommended.
- Due to mathematical reasons it is in principle more appropriate to use Gamma distributions for failure rates resp. frequencies and Beta distributions for failure probabilities instead of the lognormal distributions which have been usually applied up to now. With respect to the practical application of these distributions, however, there is still a need for investigations, e.g. concerning the transition from the lognormal distributions in the current data base to these distributions.
- In principle, mean values should be calculated as results for the frequencies of system, core and plant damage states resp. for the transition probabilities.

5.5.2 Plant design

The level 1 PSA has identified a number of problems with respect to the plant design resp. potentials for improvement, which in part are specific for the reference plant:

- The inspection periods for components of the RHR chain are not optimized.
- The contribution of transients to the frequency of core damage states can be significantly reduced by plant internal accident management measures.

- Also for LOCAs, plant internal accident management measures can be performed successfully, if suitable start criteria and procedures are inserted into the emergency manual.
- While transients contribute 96 %, and leaks 24 %, to the frequency of system damage states, leaks dominate the core damage frequency with a contribution of 78 % (transients 15 %).
- The inspection method applied in GKN 2 in order to prevent faulty calibration of transducers significantly increases the availability.
- Diversity of the batteries of the 48 V supply could significantly reduce the damage state frequencies in case of a loss of preferred power (in total approx. 10 %).
- The reliability data for the three-way-sump valve, for which operating experience is hardly available, and for the high pressure injection pumps in sump recirculation mode could be estimated only roughly, because the test conditions do not meet the requirements in case of an accident.

The results of the Level 1 PSA for power operation are affected significantly by the following problems:

- The criteria for the transition from the event oriented operating manual to the protection goal oriented operating manual have to be considerably revised.
- The „manual cool down with main steam safety valves“, included in the protection goal oriented operating manual - and other manual actions - are not trained by the operating staff.
- The measurement data logging for the ECC chain is not completely designed in reactor protection quality, the inspection periods of some of the components are too long.
- Although the 100 K/h cool down is performed automatically, the controlled main steam release due to lacking diversity of the control valves has a relatively high unavailability by CCF.

6 Level 2 PSA for normal power operation

6.1 Introduction

This section deals with the PSA level 2 for normal power operation, which covers the events from the beginning of core melting up to the release of radionuclides into the environment. The phenomena in accidents with core disruption have been investigated intensively for a long period of time. The acquired knowledge is used in computer codes for deterministic simulations of the accident progression and thus for safety assessments. These codes have been employed in the analyses performed in the present study as well.

Computer codes can be divided into codes for specific aspects, for example for the hydrogen distribution in the containment atmosphere, and into integral codes which simulate the complete accident progression, though mostly with less detail of the individual aspects. GRS predominantly employs the integral code MELCOR /NRC 97/. Examples of MELCOR-calculations are given in the following section 6.3 which deals with the accident progression after the core damage state. Relevant individual aspects are supplemented, for example by employing the code RALOC /KLE 97/ for the analysis of the containment atmosphere.

Even at the present state of knowledge and employing the most recent computer code versions, the deterministic investigation of event progressions during core melt accidents still has significant uncertainties. On the one hand, stochastic (random) phenomena are influencing the process, and on the other hand, there is uncertainty in the knowledge of many aspects. The PSA not only quantifies the frequencies of the individual event progression, but the uncertainties of the analysis results are also determined as far as possible. The world-wide common technique is the event tree analysis which is employed at GRS as well. Thereby a set of initial states – the core damage states – are put in the first part of the event tree. Thereupon follows the representation of the different possible accident progressions as a sequence of branching points together with the pertinent probabilities. Finally, the numerous possible combinations of branches are binned into final states – the so-called plant damage states.

Since the Deutsche Risikostudie Kernkraftwerke – Phase B /GRS 90/, supplementing and new knowledge has been gained for many separate aspects of accident progression. The improved computing technology now allows the analysis of more event pro-

gressions in greater detail. In addition, the knowledge of the probabilistic evaluation of not well known crucial phenomena has been developed further. This progress now allows a sound probabilistic event tree analysis of the accident progressions, although there still remains a considerable need for investigation of specific questions.

In the study presented here, this method is evaluated for the first time in Germany in a plant specific event tree analysis for core melt accidents which is as complete as possible. The probabilistic methodology employed complies with the one established by the US-study NUREG-1150 /NRC 90/. Apart from minor computational improvements, this procedure has been state of the art for the last 10 to 15 years. The procedure is characterized by a big event tree with 50 to 100 branching points and by a Monte Carlo simulation to take into account the uncertain input data and assumptions. The consultation of several experts, including external and independent individuals, as much as possible has been done frequently in NUREG-1150. But due to the considerable expense associated with this procedure, this has not been done in the present study. However, the methods required for this are at hand. They could be employed easily in a PSA if the necessary funding were available.

According to the coarse structure of an event tree, some aspects which are potentially important, for example time dependencies, cannot be represented exactly. Therefore further methodological development beyond the event tree analysis is under way, partly integrating probabilistic aspects into deterministic computer codes. These methods, however, are not yet ready for application.

6.2 Exemplary description of two accident progressions

The focus of the activities in the PSA level 1 is on the modeling of the plant systems and their failure modes and concentrates on the issue of core coolability. On the contrary, the activities in the PSA level 2 are mainly related to complicated physical and chemical processes after the core damage state, and the plant system analysis is of less importance. Accident progression simulations with integral codes are therefore an important prerequisite for the event tree analysis.

These accident progression simulations essentially show the time sequence of events. For instance, the following questions are addressed:

- How much time passes between the core damage state and the core relocation into the lower plenum?
- Will very high temperatures be reached near the load limit of primary loop components before the molten core relocates into the lower plenum?
- Is there still any residual water in the lower plenum at the time of core relocation?
- Will the filtered venting of the containment be necessary before the core melt has penetrated the concrete base mat?

According to the calculated event progressions, the structure of the event tree is set up so that it can represent the different possible progressions. To determine the individual branching probabilities, numerous additional calculated data are used, for example pressure, temperatures or inflammability. As the practically achievable number of accident simulations is much lower than the number of possible accident progressions, branching probabilities frequently have to be estimated.

Within the PSA level 2, numerous integral accident analyses with MELCOR (version 1.8.4) have been performed for the reference plant. They are described in /SON 99/ and /SON 01/. To give an impression of different accident progressions and of the range of possible progressions to be covered by the event tree, two examples of accident simulations are given:

- Slow accident evolution after core melt with low pressure in the primary system (section 6.2.1)
- Fast accident evolution after core melt at high pressure in the primary system (section 6.2.2).

6.2.1 Slow accident evolution after core melt with low pressure in the primary system

The progression after a 10 cm² leak in the hot leg with failure of low pressure emergency core cooling is a typical example of a slow accident evolution. Essential events of the accident progression are summed up in table 6.1. Heat removal through the secondary system (cooldown at 100K/h, steam relief, feedwater to the steam generators)

is available. Failure of the low pressure core cooling systems was assumed, i.e. e. water is fed into the RPV with the high pressure systems until the flooding tanks are empty.

- **Situation inside the reactor cooling system**

The core will be cooled for a long period of time because of the intact secondary heat removal system and because of the utilization of all flooding tanks by means of the high pressure safety injection system. In addition, the accumulators inject later on in the accident, so that about 17 h pass until the primary water falls below the upper level. Core melting begins at approximately 22 h.

The total amount of hydrogen produced is 670 kg, but no more than about 400 kg are released into the containment. The rest remains inside the reactor cooling system, in particular inside the empty pressurizer and in the tubes of the steam generator. Thereby, despite the heat removal via the steam generators, the pressure increases up to about 3 MPa at the time of RPV failure.

- **Situation inside the containment**

For this case a low energy input through the leak into the containment is typical. This is due to the long lasting heat removal from the reactor cooling system via the steam generators. This results in low temperatures and pressures (fig 6.1) inside the containment. The steam volume fraction in the containment is not sufficient for an inertisation. After the failure of the RPV, the pressure decreases for some time – this is typical of all cases with initially dry core-concrete interaction - and does not begin to rise again until water floods the reactor cavity after 37 h 04 min.

Table 6.1 Accident progression for a 10 cm² hot leg leak and failure of low pressure emergency cooling

Characteristic events	Time of occurrence
leak opens	0 s
Reactor scram/turbine trip	15 s
Start of shutdown with steam generators 100 K/h	22 s
Isolation of reactor coolant system, coast down of main coolant pumps, start of extra borating system	124 s
High pressure ECCS injection	3 min - 5 h 03 min
Cold leg accumulators isolated	10 min
Stop of extra borating system	1 h 57 min
Injection from hot leg accumulators	5 h 17 min - 6 h 41 min
Low pressure ECCS injection	Failure assumed
Begin of fission gas release from fuel pins	~ 21 h 30 min
Begin of core melting	~ 22 h
Hydrogen combustion in rooms adjacent to the leak	> 22 h 03 min
Melt penetrates lower core grid, begin of core relocation into the lower plenum	24 h 58 min
Dryout of lower plenum	25 h 40 min
RPV failure and melt entering reactor cavity	25 h 54 min
Hydrogen combustion in equipment rooms upon RPV failure	25 h 54 min
Melt-water-contact inside ventilation ducts	34 h 07 min
Begin of filtered containment venting	After end of calculation (>57 h)

Despite the low hydrogen release rate, the interim storage of hydrogen in the reactor cooling loop and the action of the recombiners, hydrogen deflagration prevails near the leak with flames spreading into the adjacent steam generator room above. After failure of the RPV and due to the fast release of the hydrogen which was stored in the reactor cooling loop, a hydrogen deflagration was calculated which affected additional service compartment rooms. Thereafter during an extended time period hydrogen deflagration continued to originate in the reactor cavity.

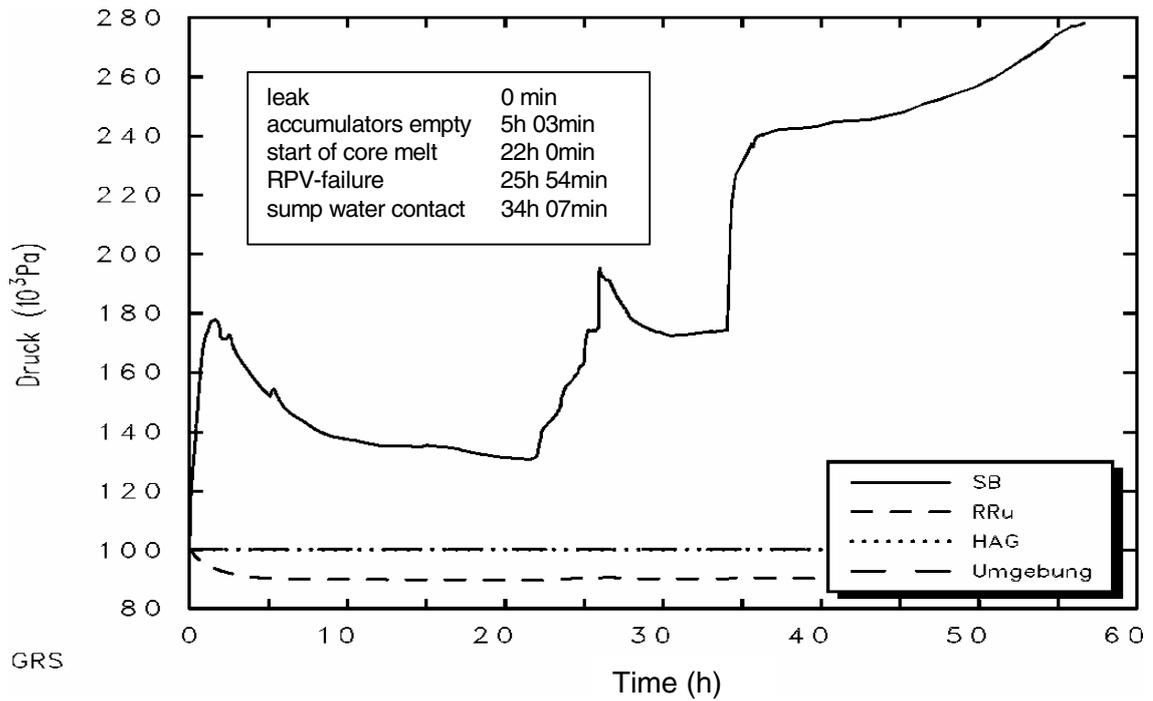


Fig. 6.1 Pressure history in containment (SB), Annulus (RRu), service building (HAG) and environment, 10 cm² leak at hot leg and failure of low pressure pumps, MELCOR 1.8.4

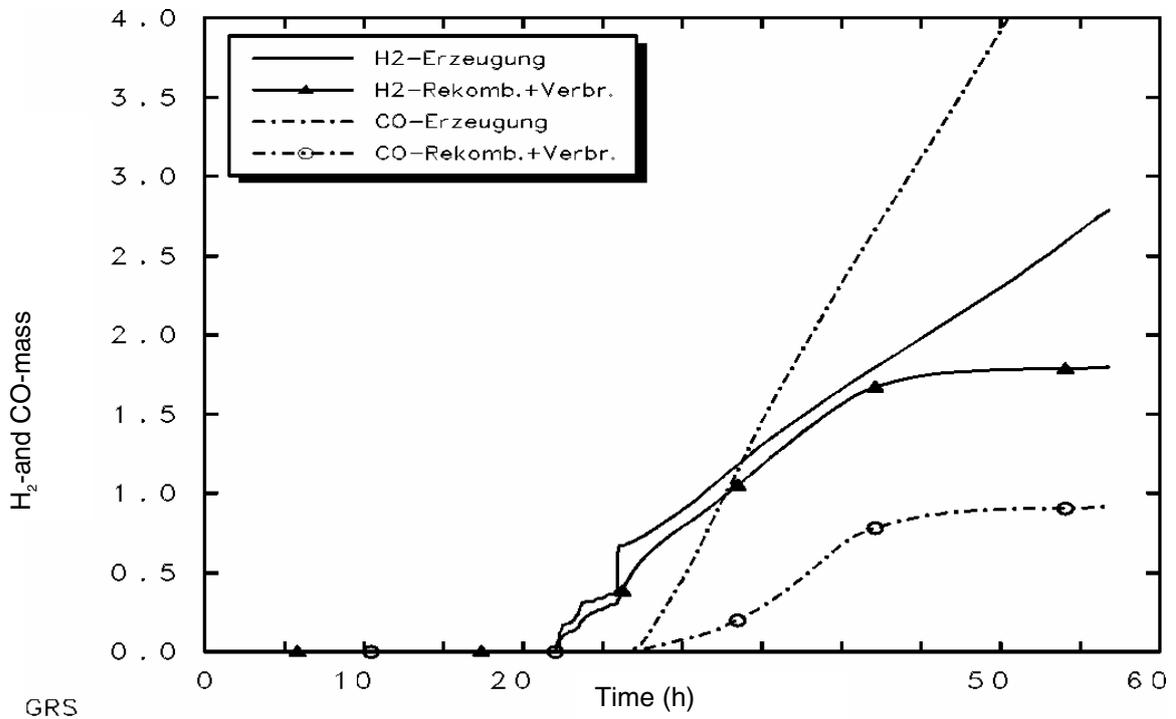


Fig. 6.2 Sum of produced and processed hydrogen and CO mass, 10 cm² leak at hot leg and failure of low pressure pumps, MELCOR 1.8.4. The hydrogen mass which is shown in fig. 6.2 reflects the process described. Before the failure of the RPV, 15 to 20 g/s of hydrogen are on average recombined, which is a

little less than the amount flowing into the containment. After failure of the RPV there is a sudden hydrogen surge and a slightly higher recombination rate as well. In the figure the burned hydrogen mass is added to the recombined mass. Later the hydrogen reduction rate matches the release rate from the core concrete interaction, which is low due to the late point in time. Because of the lack of hydrogen the recombination fades away after about 40 h. But the hydrogen and carbon monoxide generation continues.

6.2.2 Fast accident progression after core melt at high pressure

Subsequently the event progression for a transient with total loss of electric power is presented. In this event progression one perceives typical processes of a high pressure core melt accident. In this sequence it is assumed that the entire AC power supply (e.g. emergency diesel generators, supply from the neighboring unit) fails and that a recovery is not possible within the period analyzed. This consequently leads to the additional failure of the spent fuel storage pool cooling inside the containment and to an additional increase of the containment pressure due to steam from the storage pool. A decay heat of 5 MW was assumed for the stored fuel elements. With these assumptions the requirements for the pressure relief of the containment are particularly demanding. To check the performance of filtered containment venting, its correct activation at the proper pressure was assumed, though this is unlikely under the conditions of the loss of electric power.

At the time when the MELCOR-analysis was performed, preliminary estimates of the load limits for hot primary components led to the expectation that these components will fail as soon as they exceed 800 °C at a system pressure of 16 MPa. Therefore a failure of the surge line was assumed under these conditions. The structural mechanics assessments were subsequently completed with finite-element analyses before setting up the probabilistic event tree analysis. A leak in the main coolant line between 820 °C and 845 °C turned out to be the dominant failure mode. For the present purpose of the description of a characteristic event progression, the difference between a failure of the surge line and the main coolant line is not significant.

The time sequence of characteristic events is given in table 6.2.

- **Situation inside the reactor cooling system**

Simultaneously with the initiating event, the main coolant pumps coast down. Scram and turbine trip are initiated after 3.4 s by low pump speed. The steam generators are dry after about 57 min. Afterwards the pressure inside the reactor coolant loop increases and, due to the volume expansion, the water level in the pressurizer increases as well. Before the pressurizer is completely full, the pressurizer relief valve opens for the first time at 1h 06 min. A large number of valve cycles follow, by which the relief valve and later the safety valve as well limit the pressure in the reactor cooling loop. The rupture disks at the pressurizer relief tank open at 1h 28 min and the release of water and steam into the containment begins.

Table 6.2 Accident progression after transient with total loss of AC power and with consequential failure of surge line

Characteristic events	Time of occurrence
Total loss of AC power	0 s
Begin coast down of main coolant pumps	0 s
Reactor scram/turbine trip	3,4 s
Begin secondary cooldown (100 K/h)	25 s
Steam generators empty (water level < 0,1m)	57 min
Secondary bleed and passive feed from feedwater line (water level > 9 m)	dismissed
First opening of pressurizer relief valve	1 h 06 min
Rupture disc on pressurizer relief tank opens	1 h 28 min
Primary bleed	dismissed
Fission gas release from fuel rods	2 h 22 min
Begin of core melting	~ 2 h 35 min
Failure of surge line	2 h 55 min
Accumulators begin to inject	2 h 56 min
Failure of lower grid, core relocation into lower plenum	5 h 02 min
Dryout of lower plenum	5 h 04 min
RPV failure, melt entering reactor cavity	6 h 22 min
Melt-water contact in ventilation ducts	10 h 07 min
Water in fuel storage boils	~ 38 h
Begin of filtered containment venting	45 h

After about 2 h there is initial core uncover, and core heat up begins in the upper core regions. At 2 h 22 min the cladding of the fuel pins starts to break up and the collected gaseous fission products are released. Core melting begins at about 2 h 35 min in the upper core region and spreads quickly due to the high decay heat level. Thereby very hot gases are transported from the core into the upper plenum of the RPV and into the reactor cooling loop. The thin-shelled surge line reaches a temperature of 800 °C at about 2 h 55 min and fails according to the assumptions mentioned above.

The resulting pressure decrease allows the flooding of the heavily degraded core by the accumulators, which inject their total inventory into the reactor coolant loop within a few minutes. This interrupts the core melting process for some time. Up to this moment the comparatively significant amount of 520 kg of hydrogen is produced within half an hour. The release rate of hydrogen into the containment was initially determined by the pressurizer relief valve. As soon as the surge line breaks, large amounts of steam are released simultaneously together with very high hydrogen release rates (3.5 kg/s at the maximum).

In core melt accidents with high pressure there is a high probability for the availability of the electric power supply and for the availability of the emergency cooling systems. After the pressure decrease they would start injection, and depending on the extension of core damage reached so far, cooling and retention of core materials inside the RPV is possible. But at the present event progression without electrical power supply the emergency cooling systems are not available. Under this assumption the core melt process continues after 4 h 50 min. After 5 h 02 min already, the failure of the core support grid is calculated. The invading core material quickly evaporates residual water in the lower plenum, and hot gases are increasingly transported into the containment. Up to RPV failure at 6 h 22 min the total amount of hydrogen generated is 620 kg.

- **Situation inside the containment**

This class of events is characterized by a very slow pressure increase in the equipment rooms during the first 1h 30 min. This is due to the heat transfer from the main components of the reactor cooling loops and the failure of the ventilation systems. After about 30 min the pressure increase leads to the failure of some rupture foils on top of the steam generator compartments. Thus the atmospheric separation of equipment compartments from service compartments has disappeared, which consequently influences the convection inside the containment. When the rupture discs on the pressurizer relief

tank open, further rupture foils on both steam generator compartments (10 to 20 %) will fail, but the connections through the protection walls within the containment remain closed. The strong release of coolant leads to a pressure increase of up to 0.22 MPa (fig. 6.3) and to a temperature increase of up to 100 °C in the equipment and service rooms. Initially the steam volume fraction in the release room rises up to 70 %, whereas only about 50 % will be reached in the containment dome. Steam inertisation is existing but for limited periods.

Due to the failure of the surge line at 2 h 55 min there is a violent release from the reactor coolant system leading to a sudden pressure rise up to 0.43 MPa. This causes further rupture foils on the steam generator compartments (50 % to 70 %) to fail, and the rupture foils above the doors in the protection walls will be destroyed as well. Due to the ensuing good convection, the atmospheric composition in all large rooms of the containment will be mixed quickly.

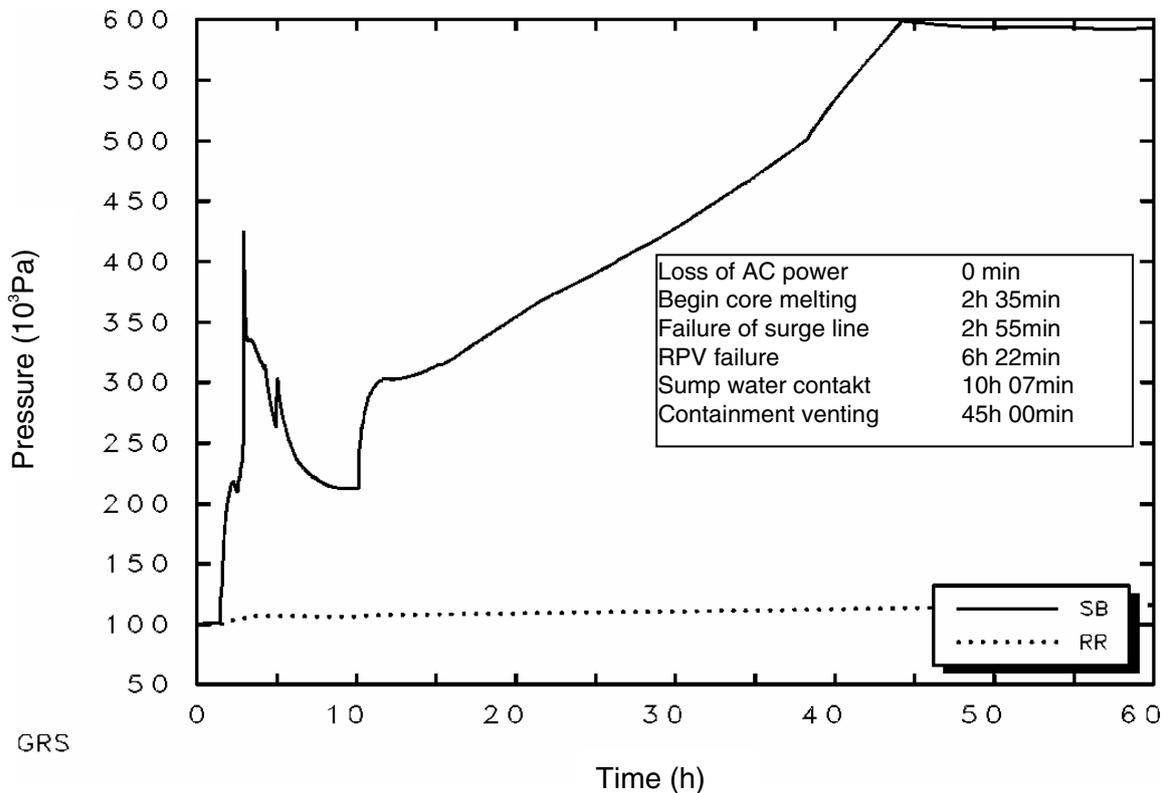


Fig. 6.3 Pressure history inside containment and annulus, total station blackout and failure of surge line, MELCOR 1.8.4

Hydrogen recombination reaches a peak value of 85 g/s due to the good convection after failure of the surge line. In particular during the phase before RPV failure, the total recombined hydrogen mass remains below the recombined hydrogen mass (fig. 6.4).

During the core-concrete interaction after 10 h 07 min (i.e. e. 3 h 45 min after failure of the RPV) there is contact between melt and water from the ventilation ducts. Due to the continuous evaporation, steam-inerted conditions begin to prevail and the pressure in the containment rises steadily. After about 38 h the pressure increase is further accelerated because at this moment the water in the fuel storage pool begins to boil. After about 44 h 15 min the pressure inside the containment reaches 0.6 MPa. At this pressure the initialization of filtered containment venting is assumed. The venting mass flow has been set at 3 kg/s, which is not sufficient to lower the containment pressure significantly under these conditions. At least the cooling of the fuel storage pool has to operate again to reach a pressure decrease. The calculation was interrupted after 60 h.

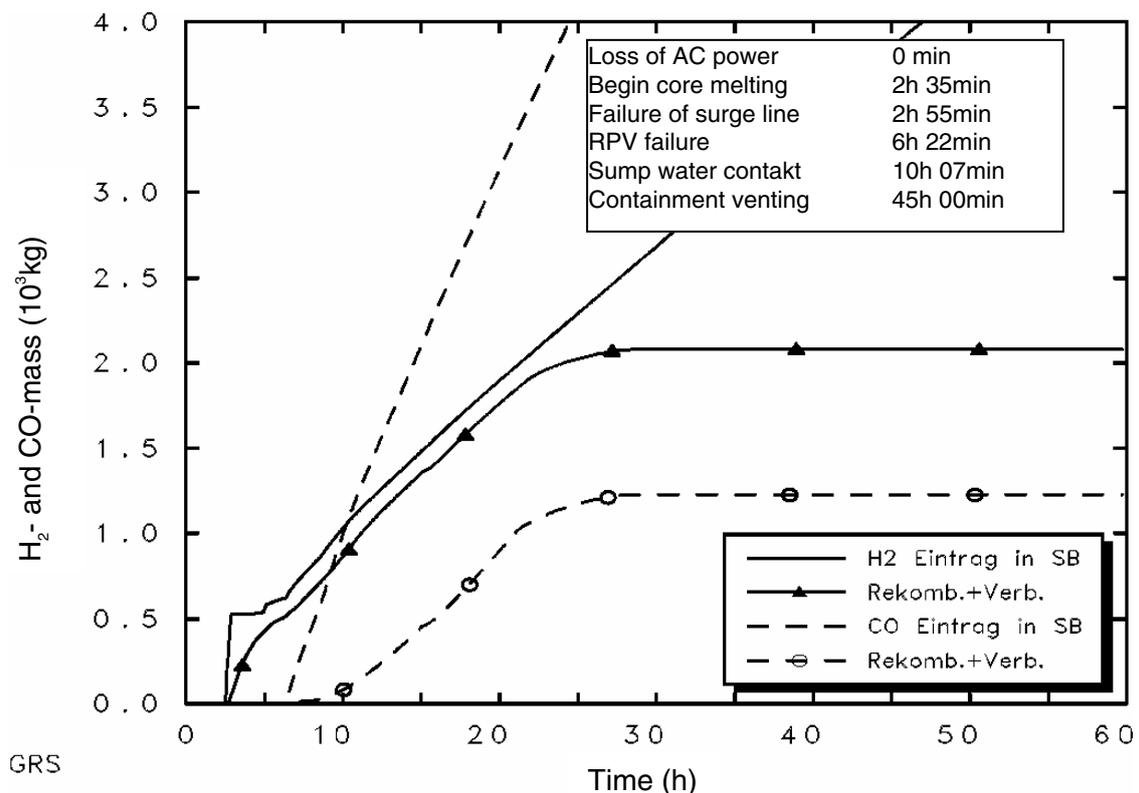


Fig. 6.4 Sum of produced and processed hydrogen mass, total station black out and failure of surge line, MELCOR 1.8.4

6.3 Event tree analysis

6.3.1 Core damage states in the event tree

For the PSA level 2 a common event tree was set up for all core damage states to allow efficient work – for example when changing input parameters or to evaluate results. However, an event tree principally has just one single initial point (the “trunk” of the tree). Therefore a procedure is required to transfer the numerous core damage states into the event tree. This procedure is presented in short below.

The characteristics and frequencies of the core damage states are given as a table. The branching points in the first part of the event tree have been used to transfer the contents of this table into the event tree (compare fig. 6.5). The first two branching points represent the number of the core damage states. The applied computer code can handle a maximum ten branches per branching point. Therefore two branching points are required to represent more than ten core damage state numbers. For example, the core damage state number 24 is assigned branch number 3 in the first branching point (representing core damage states 20 to 29) and branch number 5 at the second branching point (the fifth of the core damage states 20 to 29). With this procedure each core damage state can be identified by its number, and results of the event tree analysis (e. g. release categories) can be traced back to the individual core damage state. Thereby it is also possible to find out the underlying basic reasons at system level, because the most significant failure combinations for the core damage states are known from the PSA level 1.

The “branching probabilities” for the branches representing the numbers of the core damage states are determined so that the combination of branches exactly matches the respective core damage state’s fraction of the total frequency of all core damage states. This evaluation is done equally for each core damage state and for each sample of the Monte Carlo Simulation. The calculation does not require a significant effort if a pertinent spread sheet is applied.

Further characteristics of core damage states are inserted into the subsequent branching points of the event tree. Table 5.8 contains these characteristics, for example the initiating event or the pressure in the reactor cooling system. For each characteristic, a branching point is inserted into the event tree, splitting into the various possible states of the characteristics. If, for example, one of the core damage states is initiated by the

event “steam generator leak 1-6 cm²”, and if it has a primary pressure of 6 MPa, it is assigned a probability of 1 for “steam generator leak 1-6cm²” in the branching point for the initiating events and a probability of 1 for “pressure 1-10 MPa” in the branching point for the primary pressure. With this procedure each core damage state is assigned its characteristics in the first part of the event tree. For the number of core damage states within the PSA presented here, this procedure could be performed manually. An automatic procedure is recommended for larger numbers.

Altogether 500 000 data had to be transferred to characterize all core damage states in all 5000 Monte Carlo simulations. This transfer did not pose any technical difficulties.

For the following characteristics of core damage states, additional assumptions had to be made because they had not been considered in the PSA level 1:

- The atmospheric circulation within the containment and the ventilation of the annulus are shut down in the plant under investigation during emergency situations. Accident measures to put them into operation are not provided.
- With regard to the leak tightness of the containment is assumed that it slightly exceeds the design leakage with a leak area between 0.1 and 10 cm² and a probability between 0.0 and 0.2 (homogeneous distribution).
- The leakage feedback from penetrations of the containment back into the containment is always in operation except when the emergency electric power supply is not available. This simplistic assumption could be made because the failure of the leakage feedback falls into the same leak size category as the leakage mentioned above, but it is of a much lower probability.
- The emergency ventilation of the annulus is not operating when the emergency electric power supply is not available. In all other situations it fails with a probability of between 0.0 and 0.01 (homogeneous distribution). Failure merely means the non-function of the fan, but it does not imply an isolation of the system. Gas from the annulus can be removed under little overpressure without the fan. Therefore the influence of fan failure on the event progression is small, and the simplistic assessment of the failure probability is justified.

The event tree analysis assigns the further event progression and the frequency of various final states to each core damage state. When the event tree analysis is evaluated, the frequency of each intermediate and final result (e. g. the frequency of con-

tainment failure due to overpressure) can be traced back to any arbitrary characteristic of the core damage states (e. g. to core damage states with high RPV pressure). One of the essential objectives of this PSA is a coherent analysis right from the initiating event up to the plant damage states. Therefore the core damage states and the final states of the event tree analysis will be related to the following six groups of initiating events (compare section 5.3.4):

L<25	Leak in main coolant line with less than 25 cm ² (initiating event 4 in table 5.12)
L>25	Leak in main coolant line with 25-200 cm ² (initiating events 2 and 3 in table 5.12)
LPR	Leak at pressurizer (initiating events 5 and 6 in table 5.12)
LSG	Leak in a steam generator tube (initiating event 8 in table 5.12)
TEP	Transient together with emergency AC power (initiating event 10 in table 5.12)
T	Transient with normal AC power (initiating events 11 – 13 in table 5.12)

The further initiating events which are not mentioned here do not contribute significantly to the core damage states.

6.3.2 Set-up of the event tree

In the previous sections the definition of core damage states and the deterministic simulation of characteristic accident sequences have been explained in examples. These tasks constitute the essential prerequisites for the event tree analysis of the events from the core damage states to the plant damage states.

As previously described in the section about core damage states, the first part of the event tree is used to define the core damage states and their frequencies. Further branching points succeed which represent the analysis of the accident progression. The branching points are arranged in chronological order.

Table 6.3 Branching points of the event tree

Issues of branching points	number
Determination of core damage states (frequencies and characteristics)	17
Events between core damage state and core relocation into the lower plenum	25
Events between core relocation and RPV failure	8
Events related to RPV failure	9
Events between RPV failure and melt-sumpwater contact	4
Events after melt-sumpwater contact	11
Events outside the containment inside the annulus and inside the containment venting system	6

In addition to the 80 branching points shown in table 6.3 the event tree contains ten more branching points which serve to enter parameters for the supporting subroutines of the event tree. Beyond that, these branching points do not contribute to the structuring of the event tree.

An event tree of this size cannot be represented graphically. The principal structure of the event tree is shown in figure 6.5. There it is indicated that the event tree can be evaluated not only at its end for the plant damage states but also at every intermediate state, for example immediately after RPV failure.

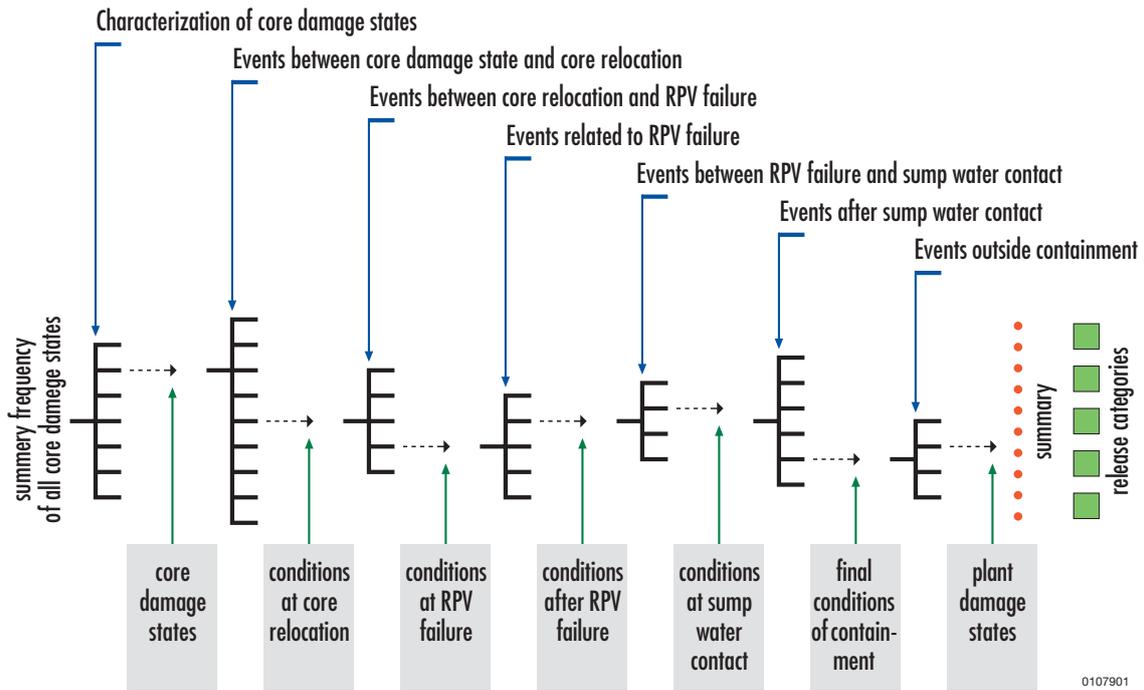


Fig. 6.5 Principal set-up of the event tree

The branching points of the event tree cover the following phenomena:

- **Incidents inside the reactor pressure vessel between core damage state (start of core melting) and RPV failure**
 - Emergency measures for pressure relief and water injection (bleed and feed)
 - Failure of components of the reactor coolant loops (main coolant line, safety valves) due to combined temperature and pressure load
 - Retention of partly damaged reactor core inside the core region or of parts of the core materials inside the lower plenum by restoration of the primary feed function
 - Fuel-coolant interaction (steam explosion) and its consequences when the core material relocates into the lower plenum
- **Incidents in the containment atmosphere before RPV failure**
 - Distribution of hydrogen inside the containment including the effect of the recombiners
 - Flammability of hydrogen mixtures, ignition sources, and consequences of possible ignitions for the containment integrity

- **Incidents related to RPV failure**
 - Time and extent of RPV failure
 - Direct mechanical consequences for the containment
 - Effect on the containment atmosphere (temperature, pressure, inflammability) and ensuing consequences for the containment integrity
- **Incidents inside the containment after RPV failure**
 - Core-concrete interaction before and after sump water contact
 - Pressure increase and atmospheric composition inside the containment, taking into account emergency measures (hydrogen recombiners)
 - Formation of containment leaks due to transgression of the load limit of the containment
 - Reliability of filtered containment venting
 - Inflammability of hydrogen mixtures, ignition sources, and consequences of ignitions for the containment integrity
 - Melt spreading at the bottom of the containment, taking into account possible damage to components (sump suction lines)
 - Penetration of concrete foundation
- **Incidents outside the containment**
 - Release paths for hydrogen and radionuclides out of containment leaks through the annulus or the auxiliary building to the environment
 - Generation and inflammability of hydrogen mixtures, ignition sources, and consequences of possible ignitions inside the annulus
 - Distribution of hydrogen and radionuclides during filtered containment venting, threat of burns inside the pressure relief system

The event tree analysis requires that even very complicated processes have to be represented by branching probabilities. These probabilities are partly calculated by dedicated subroutines in the event tree in order to evaluate them with more confidence than by merely indicating a single estimate. These subroutines, which are necessary for the

purpose of the probabilistic analysis, are a compromise between complex deterministic calculations and simplistic estimates.

For the following processes, subroutines are provided which calculate branching probabilities:

- Formation of leakages in the primary system when high pressures und high temperatures prevail
- Probability for the retention of core material inside the core region and on the core grid without significant core relocation into the lower plenum
- Occurrence and consequences of a steam explosion in the lower plenum of the RPV (see section 6.5.1)
- Inflammability of the containment atmosphere in three different locations taking into account the effect of the hydrogen recombiners (see section 6.5.2)
- Maximum pressure inside the containment including possible hydrogen burns, and possible pressure increase due to RPV failure at high pressure (see section 6.5.3)
- Time between RPV failure and the sump water ingress into the reactor cavity („dry period“)
- Conditions of the atmosphere inside the exhaust ventilation system during filtered venting of the containment (see section 6.5.7)

A more detailed description of the branching points and of the determination of the branching probabilities can be found in /LÖF 00/, /SON 01/.

The following sections contain a short summary of some significant aspects of the event tree analysis. First (section 6.4) the assessment of the pressure load limit for the containment is given because it significantly contributes to the failure probability of the containment under various conditions (e. g. due to pressure increase during hydrogen burn, or during core-concrete interaction). Thereafter, section 6.5 contains evaluations of different accident related loads of the containment.

The branching probabilities which are affected by the incidents described (e. g. the probability of leakage formation in the containment) will partly be directly inserted into the event tree and partly calculated by dedicated subroutines.

6.4 Ultimate containment strength during pressurization

After destruction of the RPV and the associated release of radionuclides into the containment, the latter represents the last remaining barrier to protect the environment. Therefore its ultimate strength under the beyond-design loads of the core melt accident is a significant issue.

Starting with the analysis results for the behavior of the containment near the failure limit /GRS 90/, analogous, very simplified estimates have been performed for the containment of the reference plant. In particular, the higher ductility of the material and the increased thickness of the steel shell have been considered.

The following parts of the containment have been analyzed:

Undisturbed steel shell with welds

Concrete embedded steel shell

Circumferential concrete floor outside the containment

Circular re-enforcement plate at the penetrations of the secondary loops through the containment

Bolted connection at the material hatch

Leak-tight box over bolted connection at material hatch

Contact with double-T-girder in the annulus outside the containment

Contact with bearing block for inspection carriage at the pole of the containment

Contact of steam line connection at the flexible joint

Possible failure modes and failure pressures due to local stress concentrations and due to the significantly increasing radial elongation of the shell in the plastic regime have been estimated for the steel shell and for geometric discontinuities. For this purpose, minimum values as well as median values from the elaborated distribution functions for yield strength and tensile strength have been employed. The maximum mate-

rial temperature of 170 °C (443 K) was assumed. It is not exceeded in any of the accident sequences which were analyzed. The elastic-plastic fracture mechanic failure criteria “flow stress” and “allowable strain” have been applied.

The failure probability has been set at zero, at a pressure of 0.774 MPa, which was the test pressure for the containment. Under continuously increasing pressure, the leak-tight box on the bolted connection of the material hatch has been identified as the weakest point of the containment. Beginning at an interior pressure of 1.04 MPa (flow stress failure criterion), a gradually increasing leak will develop which grows until the containment pressure remains stable. The values mentioned are valid for minimum material properties, which generally are assumed not to be minor with 5 % probability. For the median material properties, the respective pressure is 1.53 MPa. The knowledge uncertainty about the failure pressure of the containment has been assigned as follows: Logarithmic normal distribution, lowest value: 0.774 MPa, 5 % fractile 1.04 MPa, 50 % fractile 1.53 MPa.

When the pressure rises very fast, for example due to hydrogen combustion, the possible leak area at the leak-tight box (160 cm² at maximum) is not sufficient to stabilize the pressure. In these cases the event tree analysis employs the containment position with the lowest failure pressure for a large leak. This is the undisturbed steel shell including welds. The provisional failure mode is a limited crack along the welds. Similarly to the above procedure, the knowledge uncertainty for this failure mode can be expressed as follows: logarithmic normal distribution, lowest value 0.774 MPa, 5 % fractile 1.12 MPa, 50 % fractile 1.70 MPa.

6.5 Containment loads

The containment loads which emerge during the accident are determined by phenomena which have been under investigation for a long period of time:

- Steam explosion inside the RPV with consecutive damage to the containment
- Pressure surge inside the containment due to hydrogen burn
- Pressure surge inside the containment due to RPV failure under high pressure
- Pressure increase inside the containment due to long-term core-concrete interaction

The containment has been provided with hydrogen recombiners to prevent hydrogen burns, and filtered containment venting has been implemented to cope with the long-term pressure increase. The RPV failure under high pressure should be prevented by the emergency measure for primary pressure relief. Steam explosions have been investigated for many years with great effort, continuously improving the knowledge base to evaluate this phenomenon.

Apart from the well known “classical” containment threats, the reference plant has an additional vulnerability with regard to a possible melt attack on the sump suction lines. Moreover, filtered containment venting possibly leads to damage by hydrogen burns and to increased releases of radionuclides because the hydrogen is vented into ventilation ducts containing air, thus creating inflammable mixtures in the exhaust ducts.

The following sections summarize how the containment loads are treated in the event tree analysis. A more detailed and more complete description can be found in /LÖF 00/ and /SON 01/.

6.5.1 Impact of steam explosions inside the reactor pressure vessel

A steam explosion is a very fast or explosion-like vaporization of water upon contact with well fragmented hot core melt. It cannot be excluded a priori that a steam explosion will damage the RPV and, as a consequence, damage the containment as well. Steam explosions have been under investigation in Germany and abroad for many years. Despite these efforts there is neither a recognized computer code nor a sufficient experimental basis available to analyze with confidence the development and consequences of a steam explosion in a reactor accident.

Within PSA level 2, the development and consequences of a steam explosion often are treated by means of an expert elicitation, where probabilities for steam-explosion-related damage are estimated in a procedure which hardly can be scrutinized. This is not adequate for this complicated phenomenon. Therefore a simple subroutine was developed /LÖF 00/ for the purpose of the event tree analysis which calculates the mechanical energy release of a steam explosion. It is based on the notion of a melt jet which enters the water pool when the core material relocates into the lower plenum, where it is fragmented into particles. The subroutine at first determines the melt mass which could possibly react. Input data which depend upon the event progression (such as the melt flow rate from the core region into the lower plenum) are transferred directly

from the event tree. Input data which determine the energetics of the reaction (e. g. the size of particles generated) can be chosen by the user. These data, together with their uncertainty ranges, have been provided by an expert from the Karlsruhe Research Center (Forschungszentrum Karlsruhe).

From the mechanical loads it is derived which mechanical failures will develop. The permissible load limits for the RPV bottom and for the main coolant lines have been determined by GRS. Information about the permissible load limit of the RPV head are taken from experimental research at Forschungszentrum Karlsruhe /KRI 99/.

The result which is of prime interest is the probability of the failure of structures due to a steam explosion. This result depends in multiple ways on numerous characteristics of the accident progression, such as the prevailing pressure, the core melt mass flow rate, the assumptions about the triggering of the steam explosion, etc.

None of the numerous Monte Carlo simulations which have been performed within the event tree analysis has shown an incident which would damage the RPV head and the containment, although broad uncertainty ranges have been attributed to the input parameters.

Depending on the RPV pressure and the direction of the core relocation (radially: horizontally through the core limiter; axially: vertically through the core grid), other damage at the reactor cooling loop has emerged with the probabilities given in table 6.4.

Table 6.4 Best-estimate values of the probability for the transition from core damage states to selected damage at the reactor cooling loop due to steam explosions in the lower plenum

Core damage states	Probabilities of the transition from core damage states to damage at the reactor coolant loop due to steam explosions			
	Large leak at RPV bottom	Limited cracks at RPV bottom	Damage at primary coolant lines	No damage
Pressure inside RPV; direction of core relocation into lower plenum				
High pressure; axially	0.002	< 0.001	< 0.001	0.005
High pressure; radially	< 0.001	< 0.001	0.02	0.05
Medium pressure; axially	0.002	0.002	0.0	0.03
Medium pressure; radially	<< 0.001	<< 0.001	<< 0,001.	0.30
Low pressure; axially	< 0.001	< 0.001	0.0	0.05
Low pressure; radially	0.0	0.0	0.0	0.44
No core relocation	0.0	0.0	0.0	0.10

There is a general trend that radial core relocation is much more likely, but with less significant consequences. This is based on the fact that for radial relocation, the melt flow rate into the lower plenum is significantly restricted by flow obstacles between the core limiter and the core shroud.

The probability of damage induced by steam explosions increases with increasing RPV pressure. This is due to the fact that at high ambient pressure a comparably long period will pass before a steam explosion has to be assumed. During this period the continuous melt flow increases the mass which can take part in a reaction.

If the steam explosion leads to a large leak at the RPV bottom under high pressure, a lift-off of the RPV and an impact on the containment has to be assumed. This process however would as well take place without a steam explosion shortly after core relocation, because during the short period up to the thermal failure of the RPV no depressurization can be assumed. Therefore the failure of the RPV bottom induced by a steam explosion is no aggravation of the accident consequences which have to be expected anyway at high RPV pressure.

6.5.2 Containment load due to hydrogen

During the accident, large amounts of hydrogen are generated and released into the containment. Gas mixtures can develop which threaten the integrity of the containment if they are ignited and start burning. For this reason the plant has been equipped with passive autocatalytic recombiners which recombine hydrogen – and carbon monoxide during later phases of the accident – with oxygen. During short-term violent hydrogen ingress, in particular in early phases of the accident during the core degradation or during RPV failure, the recombiner performance might not be sufficient to prevent inflammable mixtures. During the late phase of the accident after RPV failure, inflammable mixtures are not longer possible in most cases due to the continuous oxygen consumption of the recombination process.

GRS has performed example analyses of the hydrogen removal efficiency of a system of catalytic recombiners /TIL 98/. Within this study, proposals have been developed for the system configuration and the implementation of catalytic recombiners. A simple subroutine for the determination of the containment atmosphere was developed for the event tree analysis which is based on this recombiner system /SON 99/.

In principle, the possibility exists that recombiner efficiency will be affected by accidental phenomena, for example by mechanical impacts in a loss-of-coolant accident. This was taken into account in the event tree by a pertinent reduction of the recombination rate.

If an inflammable mixture exists, there must be an ignition source as well to initiate the combustion. It is well known from accidents with uncontrolled gas release, e. g. in residential houses, that inflammable mixtures can develop without reaction over significant periods before an ignition source causes the reaction to start. In hydrogen mixtures the energy needed for an ignition is comparatively small. To take into account uncertainties, the event tree analysis employs significant uncertainty ranges for the probability of ignition sources.

Adiabatic combustion at constant volume has been taken as basis for the determination of the pressure rise due to hydrogen burns. In the event tree analysis this pressure rise is corrected by factors taking into account increased initial temperatures, incomplete combustion or inhomogeneous distribution of the reacting components

When a detonation develops, a short peak pressure exists which is higher than the adiabatic combustion pressure at constant volume. The peak pressure decreases already before the containment has reached its maximum strain. Therefore the peak pressure is not a suitable data to characterize the structural load. To define the containment load after a detonation, an effective containment pressure is introduced into the event tree analysis based on /BRE 95/. The effective pressure is the quasi-static pressure which causes the same maximal structural load as the pressure-time history of the combustion. According to /BRE 95/ a typical containment has an oscillation frequency of about 5 to 12 Hz. Fast combustions load this type of containment with a pressure which equals twice the adiabatic combustion pressure of the respective gas mixture.

Components inside the containment have oscillation frequencies up to about 100 Hz with (dampened) oscillations up to 400 Hz /BE 95/. It seems possible that some components could be torn off from their support and hit the containment under detonation loads. It is conceivable that cable routes could break and the affected cables might cause a leak at their penetration through the containment. Within the analysis performed here, these questions could not be clarified. To take into account such incidents in the event tree analysis, it is assumed that a containment leak develops with a probability between 0.0 and 0.1 (homogeneous distribution) if there is a detonation. The according leak size was assumed to fall into the range 10 to 300 cm².

The summary results of the subroutine for hydrogen distribution inside the containment are given in table 6.5. It indicates the mean probability over all core damage states for detonations or deflagrations inside the containment dome, in the compartments (periphery) between protection walls and containment shell, and in the equipment rooms. Deflagrations have to be expected with a relatively high probability. This is due to the fact that the majority of sequences involve but a minor steam inerting inside the containment and that the recombiners cannot remove the hydrogen surges fast enough which enter the containment during core degradation or upon RPV failure. Table 6.5 shows as well that detonations are almost exclusively calculated in the service compartments. In between the service compartments and the containment steel shell there are massive concrete structures. Therefore a direct damage to the containment cannot be assumed for these detonations.

Table 6.5 Best-estimate values of the probability of the transition from core damage states to hydrogen deflagrations or hydrogen detonations in selected compartments of the containment.

Occurrence of hydrogen combustion	Probability of the transition from core damage states to hydrogen combustions in:		
	Containment dome	Peripheric rooms of containment	Equipment rooms
Upon first hydrogen release into equipment rooms	Not applicable	Not applicable	det: 0.0 def: 0.34
Before core relocation into lower plenum	det: 0.004 def: 0.28	det: < 0.001 def: 0.009	det: 0.08 def: 0.30
Upon RPV failure		det: < 0.001 def: 0.14	det: 0.0 def: 0.50

det detonative
def deflagrative

RPV Reactor pressure vessel

6.5.3 Pressure rise inside the containment upon reactor pressure vessel failure

When the RPV bottom fails at an internal pressure of 8 MPa or more, it is assumed in the event tree according to analyses in /GRS 90/ that the RPV is accelerated upwards and that it will damage the containment. At an internal pressure of 2.5 MPa or less, the pressure rise in the containment at RPV failure is insignificant. Therefore a detailed analysis of sequences with pressure above 8 MPa or with pressures below 2.5 MPa is not required. Sequences with medium pressure between 2.5 MPa and 8.0 MPa need to be investigated.

When the RPV bottom fails at medium pressure, melt is ejected and fragmented into hot particles. The particles transfer heat to the surrounding atmosphere and thereby cause a pressure rise. After that, liquid water, steam and hydrogen leave the RPV. The water reacts chemically with the melt particles and produces hydrogen. If oxygen is available, the hydrogen will be ignited. The whole process is called “direct containment heating”

One prerequisite for a significant pressure rise is the existence of pathways for the melt particles where they can penetrate far into the containment compartments. In the refer-

ence plant, there are basically two ways in which the melt can be transferred from the reactor cavity to the surrounding rooms:

- Between the RPV and its supporting flange there is a steel plate which separates the reactor cavity from the reactor well. If this plate fails due to the high pressure in the cavity and due to the impact of hot particles, a free area develops for the transfer of particles into the reactor well. The fraction of melt which reaches the reactor well can be estimated according to the procedure in /PIL 96/, which has been derived experimentally. In the existing geometry, this fraction is between 7 % and 20 %. The reactor well is not isolated from the service compartments located above. Therefore it is assumed that these melt particles will reach the service rooms as well.
- Around the main coolant lines there is a gap of about 2 m² to 3.2 m² from the reactor cavity to the equipment rooms. According to /PIL 96/ this leads to melt fractions between 6 % and 8 % reaching the equipment rooms.

These minimum and maximum fractions for the transferred core material with a homogeneous distribution in between have been taken as input for the event tree. This has been used as basis for the calculation of the ensuing pressure rise. The event tree subroutine for the pressure calculation is described below.

The following assumptions have been made for the calculation of the pressure rise due to direct containment heating:

- There is an instantaneous temperature equilibration between atmosphere and melt particles in the equipment rooms and in the containment dome.
- The different pressure rise in the equipment rooms and in the containment dome due to the temperature increase, and the hydrogen ingress is distributed homogeneously inside the complete containment volume under the assumption of an isothermal change of state.

As an example, this calculation produces the results given in table 6.6.

Table 6.6 Examples of calculated states (pressure, temperature) of the containment atmosphere due to melt- and hydrogen ingress

Core melt fraction		Temperature		Resulting containment pressure (MPa)
Within equipment rooms	Within containment dome	In equipment rooms (K)	In containment dome (K)	
0	0	450	450	0.31
0.05	0.05	659	559	0.40
0.1	0.1	836	659	0.48
0.1	0.2	836	836	0.55

General assumptions:

initial pressure in containment: 0,3 MPa
initial temperature in containment: 450 K
total core melt ejected from RPV: 150.000 kg
initial core melt temperature: 3.000 K
hydrogen ejected from RPV: 400 kg

RPV Reactor pressure vessel

If the transferred mass fractions are taken which have been derived above, this example shows a pressure increase of 0.3 MPa up to about 0.55 MPa from the temperature increase alone. In this example the melt temperature has been assumed as 3000 K. According to MELCOR results, such high temperatures will not be reached. Accordingly, in the event tree the melt temperature upon RPV failure is a homogeneous distribution between 1800 K and 2800 K. Therefore the table 6.6 is an upper estimate for the pressure increase due to melt ingress.

The hydrogen mass which enters the containment comes from the mass which was accumulated in the reactor coolant loop and the mass which is generated in addition when the RPV fails. The latter can be generated for example when water from the accumulators is released after the RPV failure. Both hydrogen contributions are estimated on the basis of MELCOR results /SON 99/. The mass which is accumulated inside the reactor coolant loop at 16 MPa is about 200 kg. The additionally generated mass is estimated between 200 and 600 kg (homogeneous distribution) for RPV pressures above 2.5 MPa.

For the calculation of the inflammability it is assumed that the hydrogen mass is released exclusively into the component rooms. The inflammability is determined with this assumption and for the atmospheric conditions which prevail after the melt particles have entered the containment. The hot particles are continuously acting as ignition

sources. The development of a detonative hydrogen concentration has not been assumed because before that, a deflagration would occur.

The last phase of the ejection from the RPV bottom consists of the residual steam mass until pressure equilibrium is attained. The additional pressure rise in the containment due to the steam flow from the large leak at the RPV bottom is estimated according to the pressure increase for the initiating event "large leak at a main coolant line". The lower pressure inside the RPV which prevails here compared to the initiating event is taken into account.

In conclusion, the mean probability of a thermally-induced RPV bottom failure at medium pressure is about 33 % of all core damage states. In about 0.6 % of all core damage states, a pressure develops which is higher than the ultimate capacity of the containment strength. Despite this very low probability the process has to be taken into account for the further analysis because it leads to a significant radionuclide release into the environment.

6.5.4 Melt spread in the lower part of the containment

At the bottom of the concrete support cylinder for the RPV there are 8 pressure equalization flaps which will open if there are any accidental pressure differences (fig. 6.6). It follows that the water from the containment sump will flow into the annulus between the RPV support cylinder and the biological shield.

About 0.75 m above the bottom of the reactor cavity there is an opening for inspection (area about 0.7 m x 0.7 m). It is closed by a removable plug which is filled with concrete. This plug is sealed, so that no sump water can enter the cavity through this path.

About 0.7 m below the bottom of the cavity there are ventilation ducts in a star-like pattern to remove heat from the biological shield. The ducts are connected to openings at the bottom of the annulus between the RPV concrete support ring and the biological shield. Because water has to be assumed inside this annulus in an accident (see above), water will enter ventilation ducts as well.

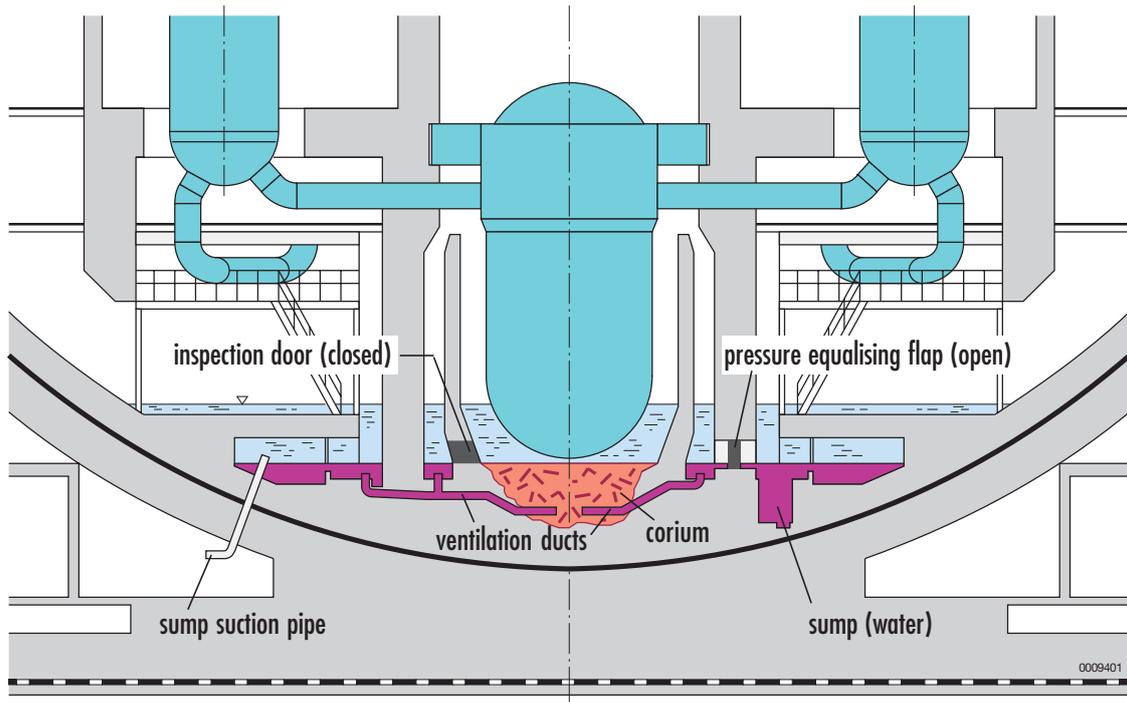


Fig. 6.6 Core melt in the lower part of the containment

When the melt erodes the concrete and penetrates into this network of ducts, melt will flow towards the containment sump. The melt will reach the steel sheet ducts which rise vertically at the inside of the containment sump. Although they are surrounded by water at the outside, the thin sheet will probably not pose any significant obstacle for the melt. After the failure of the steel ducts the melt will reach the sump region.

It is important for the further event progression whether the melt will reach the suction pipe stubs of the emergency core cooling systems. The area available for melt spread at the bottom of the sump is approximately 200 m². If the melt were a dense slab, it would surround the pipe stubs with a layer about 65 mm thick.

Additional estimates with the code LAVA /ALL 99/ have been performed to find out how far such a thin layer of melt could flow in the sump area. The code was developed at GRS to analyze the spread of core melt as a layer and in ducts. The code calculates that the melt will cover the whole sump area about 5 to 6 s after it enters the ventilation ducts. At the front, which contacts the pipe stub, the temperature still will be about 2250 K, and the liquid volume fraction there will be about 75%. Although these calculations contain significant simplifications, in particular with regard to an ideal geometrical

model, one can conclude that a thin (several centimeters) liquid melt layer can spread under water over a distance of some meters without losing much of its flowing ability.

Experimental results of the core-concrete interaction under water show the generation of voids inside the melt due to the formation of stable crusts, the existence of particle beds with a much lower density than compact core material, or the local accumulation of frozen melt in volcano-like shape. For example, in the test MACE M3b /FAR 97/, with a bottom area of 1.2 m x 1.2 m and an initial melt depth of 0.2 m, a particle layer developed within 6 h whose surface was elevated about 0.15 m above the initial melt level. In addition, a “volcano” developed, whose “peak” rose about 0.4 m above the water level. Therefore it can be assumed that the mean surface level of the core materials will be significantly higher than that of a theoretically dense core melt.

Under the conditions described above, the lower part of the sump suction pipes will be surrounded by core material whose surface level will be significantly higher than the theoretical 65 mm. 0.2 m are assumed in figure 6.7. Yet a direct flow of core material into the pipes cannot be assumed because the opening of the pipes is located about 0.6 m above the sump bottom.

6.5.5 Load and failure of sump suction pipes

The calculations with the code LAVA mentioned above have shown that the core melt spreads swiftly at the bottom of the containment sump and reaches the sump suction lines shortly after. The outer protection tube of the sump suction line (see fig. 6.7) will consequently be loaded with hot core material, while being surrounded by sump water above.

When there is an interaction between core melt, concrete and water, a large quantity of particles will be generated with a broad particle size spectrum. Small particles can float in the water for some time, or be whirled up repeatedly. When they settle, they also reach the opening of the sump suction pipes. Because these processes last for a comparatively long period (several days), small settling mass flows could also accumulate significant amounts of core material inside the sump suction pipes. The probability of the ingress of considerable masses of core material into the sump suction pipes seems to be small, but not negligible.

The particle bed which develops at the bend of the sump suction line outside the containment will initially be water-cooled. By transferring estimates for the coolability of flat particle beds to this geometry, it can be expected that the particle bed will begin to boil and dry out, leading to a non-coolable configuration. Therefore the failure of the sump suction pipe which is filled with hot core material and surrounded by the annular gap has to be assumed with high probability. After that, the core material must penetrate the protection tube before it reaches the annulus, thus eliminating the barrier function of the containment. For the protection tube the load is similar to those of the sump suction pipe, therefore its failure has to be expected as well. Thereafter sump water, core material and the containment atmosphere including hydrogen enters the annulus.

According to the estimates described above, the probability of a failure of at least one sump suction pipe is assumed to be between 0 % and 10 % (homogeneous distribution) for sequences with core melt at the reactor cavity.

6.5.6 Erosion of the concrete foundation

According to existing experimental evidence in the event tree, an end of the core-concrete interaction before penetration of the foundation is not implemented. This means that gas from the interaction keeps being released. A considerable part consists of noncondensable gases (e. g. hydrogen, carbon monoxide), leading to a continuous pressure increase inside the containment until the pressure relief has to be activated. At the same time this means that all sequences with failure of the RPV lead to a penetration of the melt into the ground.

The velocity of the erosion primarily depends on the heat flux from the melt downward into the concrete. This is in itself dependant on the decay heat and thus on the time period since reactor shutdown. Uncertainties are due to the fraction of radionuclides

which will leave the melt and the partition of the heat flux to the bottom and to the top. Table 6.7 contains information about times which pass until certain erosion depths (to the ventilation ducts, to the containment steel shell, to the ground) are reached. The values in the second line of the table are typical time periods; the first line (bold numbers) contains the pertinent probabilities (mean over all core damage states). There is a pit at the bottom of the sump where the concrete is thinner than elsewhere (see fig. 6.6). This has been taken into account for the time values given.

Table 6.7 Probabilities for the erosion of the concrete foundation due to core melt

Phase of concrete erosion	Probability (first lines) and times (second lines) of the transition from core damage states to various depths of concrete erosion			
„Dry period“ after RPV failure before core melt reaches the water filled ventilation ducts	0.06 < 5 h	0.32 5 - 20 h	0.30 20 - 100 h	0.32
Time between core damage state until melt reaches the containment steel shell embedded in concrete	0.20 < 1 day	0.46 1 – 5 days	0.02 > 5 days	RPV intact
Time between core damage state until melt reaches the ground	0.29 < 5 days	0.32 5 - 15 days	0.07 > 15 days	

RPV Reactor pressure vessel

6.5.7 Filtered venting of the containment

The successful initiation of filtered venting depends on the proper function of the venting valve and some further components and on the correct action of the staff. Failure due to loss of electric power is not considered in the event tree analysis because pressure relief of the containment is necessary no earlier than one day after the initiating event. During that period a successful reestablishment of the electric power supply is assumed. A fault tree analysis has been performed to analyze the failure of technical components. The human performance has been estimated by a qualitative and quantitative assessment of human action. /SON 01/. The analysis came to the conclusion that the mean value of the non-availability of pressure relief is 0.04 (logarithmic normal distribution; the 0.05/0.95 quantiles are 0.02/0.081). This means that of those 68 % of core melt sequences where venting of the containment is required, a fraction of 4 % (mean value) will not succeed. In the event tree analysis a consequential failure of the containment due to overpressure has been assumed. This is a pessimistic assumption

because considerable time will be available for another attempt between the criterion for the initiation of pressure relief and the containment failure pressure.

When venting has been initiated there is gas mixture inside the containment which mainly consists of steam, hydrogen, nitrogen and carbon monoxide. The oxygen has been used up due to the effect of the recombiners and/or due to combustions. Therefore the mixture is not inflammable inside the containment although it contains high fractions of gases which generate inflammable mixtures together with air.

Upon venting, the containment atmosphere is directed through the venting line into the venturi scrubber, where the steam fraction will be condensed. Thereby the fraction of the noncondensable gases is increased. For example, the volume fraction of hydrogen together with that of carbon monoxide reaches approximately 50 %. These gases are then blown into the exhaust ventilation duct on the roof of the auxiliary building. This ventilation duct comes as a vertical pit from the compartment housing the fans and it is deflected horizontally in a rooftop compartment into the exhaust duct leading to the stack. If the hydrogen-containing gas mixture from the venting system forms an inflammable mixture together with the air in the exhaust duct and if there is an ignition source, combustion will occur in the exhaust ventilation system.

There are no real indications for the existence of ignition sources in the ventilation ducts. Taking this into account, one could assume a low probability of an ignition. But hydrogen mixtures are prone to ignitions already by small-scale local effects (e. g. when a flow is bent around a sharp edge). As containment venting will last for many hours and highly inflammable mixtures will develop, an ignition is not unlikely. Therefore an ignition probability in the exhaust duct has been assumed to be between 0.0 and 0.5 (homogeneous distribution).

After a first ignition and combustion in the exhaust duct, hot spots and glowing residuals will remain. Even if containment venting were to be interrupted for some time, another ignition would therefore have to be assumed upon restart of the venting process. As a consequence, combustions on the roof of the auxiliary building lasting for hours have to be taken into account. The roof area is not protected against fire as a consequence of external events, e. g. due to an aircraft crash. Therefore consequential damage must be expected, for example at the door from the exhaust duct to the rooftop of the auxiliary building or at the entry of the line to the stack. The spreading of the fire, for example due to heat impact, ignited isolation material or hot debris falling from the roof,

cannot be excluded. It has to be taken into account that the fire is linked to a severe general condition of the plant, so that efficient fire fighting is very uncertain. Perhaps fire-related damage could develop at the scrubber of the venting system or at its pipe connections.

If the operation of the ventilation system in the auxiliary building remains uninterrupted, the fire cannot spread upstream through the ventilation ducts into the auxiliary building. But short term interruptions of the volume flow, which can easily be imagined under such disturbed plant conditions, could enable a fire to spread into the building. Without an in-depth analysis a quantitative estimate of the consequences is very uncertain. There could be an influence on the release of radionuclides if sections of the venting system located inside the building were damaged... In this case the release would bypass the filter of the venting system.

The event tree analysis requires the probability of a consequential failure of the venting filter in order to assess the release of radionuclides into the environment. According to the considerations above, a filter failure seems to be unlikely. But the discussion has shown that the consequences of a fire on the roof of the auxiliary building are very uncertain. Therefore a probability between 0.0 and 0.2 (homogeneous distribution) has been assumed for the filter failure due to a fire.

6.6 Results of the event tree analysis and their relation to initiating events

The characteristic results of the event tree analysis are given in the following tables:

- Final location of the core materials (table 6.8)
- Pressure inside the reactor coolant loop immediately before RPV failure (table 6.9)
- Final status of the containment (table 6.10)
- Release paths for radionuclides into the environment (table 6.11)
- Release categories for radionuclides (table 6.12)

The tables show how the accident progresses depending on various initiating events. The initiating events are binned as follows:

- L<25 Leak in main coolant line with less than 25 cm
- L>25 Leak in main coolant line with 25-200 cm²
- LPR Pressurizer leak
- LSG Leak in a steam generator tube
- TEP Transient together with emergency AC power
- T Transient with normal AC power

6.6.1 Final location of the core materials

Table 6.8 summarizes the conditional probabilities of the transition from initiating events to the different locations for the final location of the core materials.

The core material can be retained in the original core region or in the lower plenum inside the RPV if during the course of core degradation a primary feed function is initiated just in time. A feed function is particularly likely if the feeding systems cannot inject in the core damage state because primary pressure is too high, and if later a leak in the primary loop causes the pressure to decrease. This sequence has to be expected in particular for transients. In most other sequences there is no injection, so that a failure of the RPV bottom due to core melt impact cannot be avoided.

Table 6.8 Probability of the transition from core damage states to different final locations for core materials

Final location of core materials after core damage states	Probability of the transition from core damage states to final locations of the core material for different initiating events (designation, fraction) ¹⁾							
	Initiating event fraction of CDS	L<25	L>25	LPR	LSG	TEP	T	Mean over all CDS
In core region (no RPV failure)		0.016	0.04	0.035	0.006	0.001	0.004	0.102
In lower plenum (no RPV failure)		0.114	0.02	0.025	0.003	0.013	0.04	0.215
Outside RPV		0.40	0.04	0.09	0.061	0.086	0.006	0.683

RPV Reactor pressure vessel CDS core damage state
T Transient LSG Steam gen. tube leak
TEP Transient with emergency AC power LPR Leak at pressurizer

6.6.2 Pressure inside the reactor coolant loop immediately before RPV failure

High pressure in the RPV can already exist in the core damage state (26 % of all core damage states are high pressure sequences). High pressure can develop during or after core degradation, in particular when the core material falls into the residual water inside the lower plenum. The degree of this pressure surge, its duration and the pressure which still prevails when the RPV fails are uncertain.

The pressure inside the reactor coolant loop can decrease shortly before RPV failure due to active pressure relief, due to a leak in a hot line, or due to a stuck-open valve.

Table 6.9 Probabilities of the transition from core damage states to the RPV pressure shortly before RPV failure for different initiating events

RPV pressure short before RPV failure	Probability of transition from core damage states to RPV pressure short before RPV failure for different initiating events (designation, fraction)						Mean over all CDS
	L<25	L>25	LPR	LSG	TEP	T	
Initiating event fraction of CDS	0.53	0.10	0.15	0.07	0.10	0.05	
High pressure (> 8 MPa)	0.01	<<	<<	0.016	0.01	0.003	0.039
Medium press. (2,5 - 8 MPa)	0.424	0.003	<<	0.019			0.446
Low pressure (> 2,5 MPa)	0.096	0.097	0.15	0.035	0.09	0.047	0.515

RPV Reactor pressure vessel CDS core damage state
T Transient LSG Steam gen. tube leak
TEP Transient with emergency AC power LPR Leak at pressurizer

Fig. 6.8 shows in principle the contributions of the different effects to the pressure decrease or increase up to RPV failure. The figure has different pressure levels (10 MPa or 8 MPa) for the lower limit of the high pressure cases. This is due to the fact that for the core damage state, the pump head of the safety injection pumps (10 MPa) is important, while at RPV failure the pressure limit for a lift-off of the RPV (8 MPa) is decisive. This figure 6.8 shows that the data for the RPV pressure given in table 6.9 is but rough information.

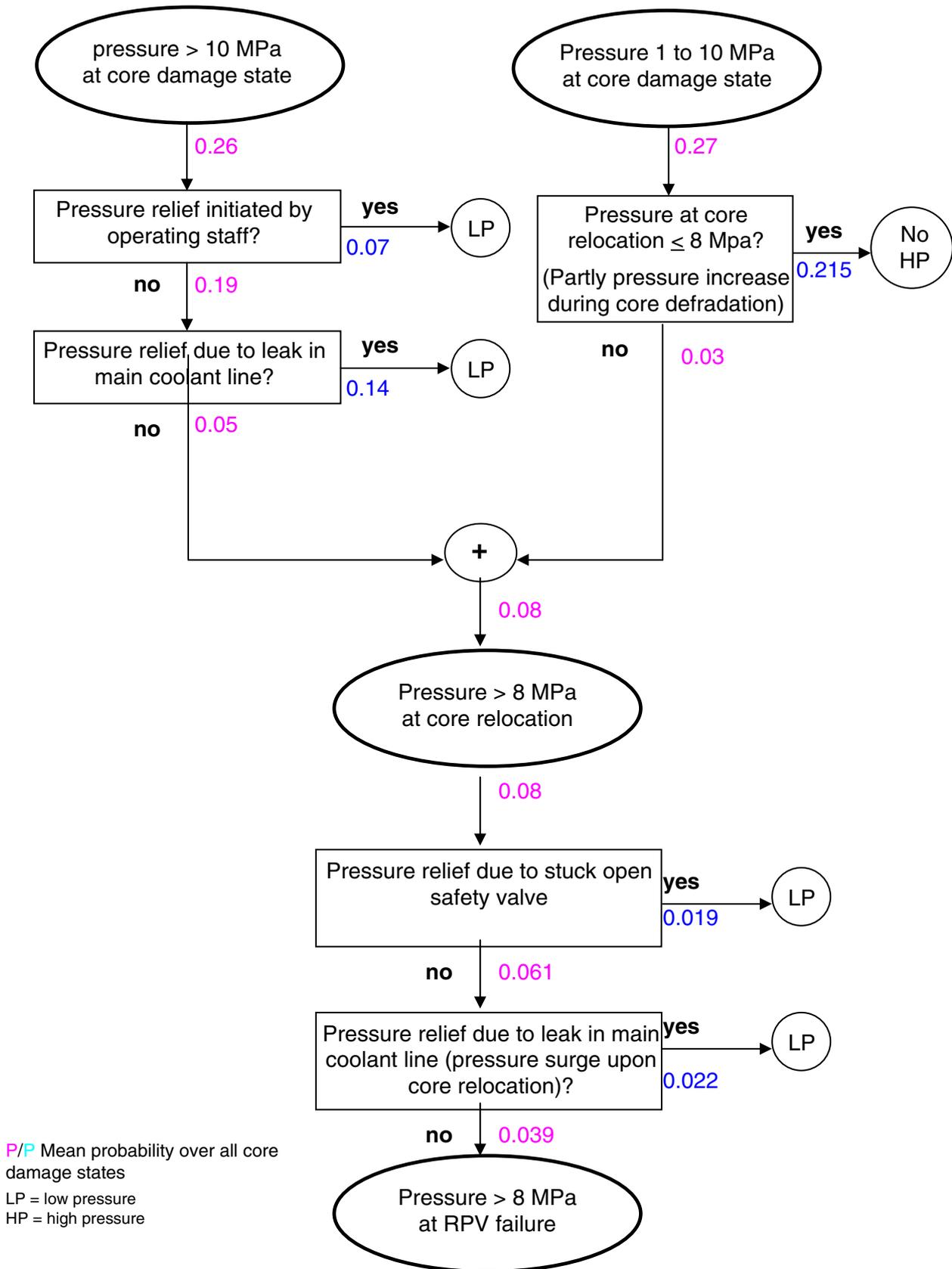


Fig 6.8 Principal representation of the pressure evolution in the reactor coolant loop from core damage states until RPV failure

6.6.3 Final status of the containment

Table 6.10 summarizes the probabilities of the transition from initiating events to final states of the containment.

If there is an RPV failure at high primary pressure – i.e. for transients without pressure relief or for small primary leaks with pressure increase during core degradation – and if the failure area is large, one has to assume that the containment will be damaged.

The failure probability of the containment ventilation isolation is insignificant for all initiating events.

When the RPV bottom fails under medium pressure, a consecutive failure of the containment due to direct containment heating is very unlikely.

For all core damage states there is a small but significant probability of the failure of the containment function due to the melt-through of a sump suction line or due to a failure of the containment pressure relief system.

Pressure relief of the containment is always required when the core material cannot be retained inside the RPV. Therefore the most likely final status of the containment is filtered containment venting, except for transients.

If the RPV does not remain intact, a core-concrete interaction will take place. Based on present knowledge, a coast-down of this reaction cannot be assumed. Therefore all sequences with failure of the RPV finally will involve a penetration of the concrete foundation as well.

Steam explosions or hydrogen burn have turned out to be insignificant contributions to containment failure. Therefore they are not mentioned explicitly in table 6.10.

Table 6.10 Probabilities of the transition from core damage states to final states of the containment for different initiating events

Final status of containment	Probability of transition from core damage states to final status of the containment for different initiating events (designation, fraction)							
	Initiating event fraction of CDS	L<25	L>25	LPR	LSG	TEP	T	Mean over all CDS
Damage due to high pressure RPV failure	0.01				0.016	0.01	0.003	0.039
Containment isolation fails								
Failure due to direct containment heating	0.005				0.001			0.006
Melting of sump suction pipe	0.02	0.002	0.005	0.024	0.004			0.055
damage due to overpressure after failure of venting	0.02	0.002	0.005		0.004			0.031
Intact with venting	0.345	0.036	0.08	0.02	0.068	0.003		0.552
Intact without venting (core material inside RPV)	0.13	0.06	0.06	0.009	0.014	0.044		0.317

RPV Reactor pressure vessel

T Transient

TEP Transient with emergency AC power

CDS core damage state

LSG Steam gen. tube leak

LPR Leak at pressurizer

6.6.4 Release paths and release categories for radionuclides

The consequences of the accident outside the plant depend in the first place on the amount of radionuclides released. For the evaluation of the release, the status of the containment described above as well as the release paths given in table 6.11 are significant. In the first column the table contains the names (FKA to FKJ) of the release categories appearing in this study. Names FKD and FKG were intended for containment bypass sequences to the annulus, but they do not appear in table 6.11 because of their vanishing frequency. The following columns contain the release path to the atmosphere, the fractions of some selected radionuclides which are released, and the contributions of the individual initiating events to this release category.

The three rightmost columns show the results of the uncertainty analysis for the frequencies of the release categories: mean values and the 5 %-, 50 %- and 95 %-quantiles. These quantiles are an indication of the degree of confidence. As an example, for release category FKA, there is a degree of confidence of 95 % (and 50 %, re-

spectively) that it has not a higher frequency than $8.6 \cdot 10^{-7}/a$ (and $0.52 \cdot 10^{-7}/a$, respectively). The mean value for FKA is $2.1 \cdot 10^{-7}/a$.

When the RPV bottom fails under high pressure, not only damage to the containment, but also damage to the annulus has to be taken into account. Therefore the radionuclides are released directly from the RPV into the environment (FKA). When there are less energetic incidents – e. g. the melt-through of a sump suction line – the radionuclides from the containment flow into the annulus, which is initially intact. Overpressure develops in the annulus, and the first components to fail are probably the flaps of the operational ventilation system. Therefore, after a certain residual time, the radionuclides will flow through the ventilation ducts into the environment without being filtered (FKE). If the leakage from the containment to the annulus is low, the filtered emergency ventilation system in the annulus is sufficient. In this sequence the radionuclide release is low (FKJ).

During filtered containment venting, fire can cause damage to the ventilation exhaust system. Depending on the kind of damage, the radionuclides will be released at stack (FKI) or roof level (FKH). If the venting filter as well is damaged by the fire, the release is unfiltered (FKF).

The behaviour of the radionuclides during the different phases of the accident has been estimated primarily on the basis of MELCOR-results. Table 6.11 contains the fractions of the core inventory which will be released to the atmosphere for the noble gases (krypton, xenon) and for the radiologically important elements cesium und iodine.

In general, there is a trend to lower frequencies with increasing consequences. Filtered sequences (FKH, FKI, and FKJ) amount to about 75 % of all events. The unfiltered releases mainly (18 % of all events) are late in the accident evolution. There remains a fraction of 8 % of all events with very high and early releases. The main contribution comes from the steam generator tube leak with an uncovered leak and from sequences with a high pressure failure of the RPV.

Table 6.11 Probabilities of the transition from core damage states to release categories and uncertainty ranges for the frequencies of release categories

Release categories				
Name	Release path to atmosphere ¹⁾	Released fractions		
		Kr, Xe	Cs	J
FKA	Cont → damaged annulus → environment <i>or</i> release through uncovered SG tube leak	~ 1.0	> 0.5	> 0.5
FKB	Cont → non-isolated Cont ventilation → environment <i>or</i> Cont → ann. early → ann. ventilation. → envir.	~ 1.0	0.13 ... 0.24	0.14... 0.23
FKC	Release through covered SG tube leak	~ 1.0	0.02 ... 0.05	0.015
FKE	Cont → ann. late → ann. ventilation → environment	~ 0.9	2.4E-4 ... 6E-3	0.055
FKF	Cont → venting at roof level with filter failure <i>or</i> increased cont leakage → ann. → environment	~ 0.9	6E-6 ... 1.2E-4	0.0275
FKH	Cont → filtered venting at roof level	~ 0.9	2E-7 ... 1E-5	0.0001
FKI	Cont → filtered venting at stack level	~ 0.9	2E-7 ... 1E-5	0.0001
FKJ	Cont leakage as designed → filtered annulus ventilation	~ 0.9	3E-10 ... 2E-8	0.0001

1) all release categories except FKJ have additional ground contamination

RPV Reactor pressure vessel CDS core damage state
T Transient LSG Steam gen. tube leak
TEP Transient with emergency AC power LPR Leak at pressurizer

If the leak position of a steam generator tube leak is below the water level, the release is much lower (FKC) than with an uncovered leak (FKA). Primary pressure relief could significantly reduce the release, in particular for sequences with an uncovered tube leak. But there remain uncertainties with regard to the feasibility of primary pressure relief under the conditions prevailing here. In addition possible unfavorable consequences (e. g. sudden release of hydrogen from the rupture disc of the pressurizer relief tank into the steam-free and therefore non-inerted containment) have not yet been studied in sufficient detail. For these reasons, primary pressure relief has not been taken into account for a steam generator tube leak. Because the accident

Table 6.12 Frequency of release categories and probabilities of the transition from

Release categories		
Name	Main reason for release ¹⁾	frequency (10 ⁻⁷ /a)
FKA	High pressure RPV failure <i>or</i> Bypass through uncovered SG tube leak	2.1
FKB	Failure to isolate containment ventilation	0.13
FKC	Bypass through covered SG tube leak	0.23
FKE	Failure of sump suction tubes <i>or</i> failure of containment venting	1.4
FKF	Failure of venting filter due to hydrogen combustion <i>or</i> leak in annulus due to hydrogen combustion	2.1
FKH	Ventilation duct failure at venting system due to hydrogen combustion (filter intact)	2.6
FKI	Containment venting as designed	8.8
FKJ	Containment function within design range	7.7

1) all release categories except FKJ have additional ground contamination

RPV	Reactor pressure vessel	CDS	core damage state
T	Transient	LSG	Steam gen. tube leak
TEP	Transient with emergency AC power	LPR	Leak at pressurizer

The following relations can be realized:

- The release category FKA ensues from core damage states with high pressure (RPV failure at high pressure) and medium pressure (in particular uncovered steam generator tube leaks).
- Release category FKC, which exclusively ensues from the steam generator bypass with water covering the tubes, has medium pressure in the core damage state.

core damage states to release categories

Probability of transition from core damage states ²⁾ to release categories						
Number ³⁾ , primary pressure, time, frequency						
2	3	4	5	6, 7, 8	9	10, 11
LP	LP	MP	MP	MP	HP	HP
2 - 4 h	4 - 12 h	< 2 h	2 - 4 h	> 4 h	< 2 h	2 - 4 h
2.8E-7	8.7E-7	2.7E-7	9.5E-8	3.1E-7	3.1E-7	3.5E-7
0.0				0.51	0.06	0.07
	0.012					0.004
0.0	0.0	0.0	0.0	0.077	0.0	0.0
0.10	0.10			0.013		0.06
0.02	0.027					0.51
0.21	0.20			0.03		
0.67	0.65			0.10		0.0
0.0	0.0	0.93	0.82	0.25	0.81	0.34

2) compare table 5.11
 HP high pressure
 MP medium pressure

3) compare table 5.8
 LP low pressure

- Release category FKE, with a late failure of the containment, partly ensues from loss-of-coolant accidents (low pressure) and partly from transients (high pressure), which involve a passive pressure relief of the reactor coolant system, but without function of the emergency core cooling system.
- Release category FKF is mainly due to low pressure sequences where the filter of the containment venting system is damaged by hydrogen fire. Part of FKF comes from transients (high pressure) with station blackout when the leak control system at the penetrations of the containment does not work, and when this leakage leads to hydrogen combustion inside the annulus.

- Release category FKI is related to the correct operation of the containment venting system. It is attributed to all sequences that involve a failure of the RPV, as long as there is no incident which causes higher releases.
- Release category FKJ is due to high pressure and medium pressure core damage states which are converted to low pressure cases after a pressure relief of the primary system and where the operation of the emergency core cooling systems prevents the core materials from penetrating the RPV.

6.7 Uncertainty of results

The uncertainty analysis of the event tree evaluation has been done with the code package SUSA /KLO 99/. It deals with uncertain knowledge (known as epistemic uncertainties) and employs a Monte Carlo simulation. The sample size was 5000; i.e. e. 5000 evaluations of the event tree have been done with different values of the epistemic uncertainties. These uncertainties are transferred into uncertain input data of the event tree. The degree of knowledge was represented by subjective probability distributions. Examples can be found in the discussions of section 6.5.

Within the level 2 of the PSA, subjective probability distributions have been assigned to 120 uncertain input data. Phenomena with particularly numerous uncertain data are hydrogen issues (e. g. ignition probabilities or parameters governing the hydrogen distribution inside the containment) and the pressure load of the containment (e. g. loss of coolant, hydrogen combustion, core-concrete interaction). A more detailed description of the uncertain input data together with the specified distributions can be found in /LÖF 00/.

In addition, uncertainties from the PSA level 1 were included into the event tree analysis. A set of 5000 samples was transferred to level 2, which contained the subjective probability distribution for the expected frequencies of the core damage states. This procedure makes it possible to evaluate the epistemic uncertainty of the final results, e. g. of the frequencies of the release categories, with regard to the contributions from level 1 as well as from level 2.

Apart from the input data described above which contain subjective probability distributions, many input data were represented merely by point values. These data are either well known, or their uncertainty was assessed to be of minor influence on the results of

the PSA level 2 or on its uncertainty. /LÖF 00/ contains an overview of these input data without uncertainty ranges.

Table 6.11 contains the 5 %, 50 % and 95 % quantiles of the subjective probability distributions for the expected frequencies of the release categories. The ratio between the 95 % quantiles and the 5 % quantiles is higher for the less frequent and more severe categories than for the more frequent and less severe categories. As an example, the ratio for release category FKA is about 340, while it is about 40 for FKJ. This reflects the fact that the evaluation of very rare and severe phenomena has a higher epistemic uncertainty than the evaluation of more frequent and less severe consequences.

Figure 6.9 is a summary of the results of the Monte Carlo simulation. It contains the subjective probability distributions for the expected frequencies of the release categories. The figure shows the 5 %, 50 %, and 95 % quantiles and the expectation value (mean value) of the calculated frequencies. As an example, the expected frequency of release category FKA is below $8.6 \cdot 10^{-7}/a$ in 95 % of all simulations. This is similar to the statement that the expected frequency is below $8.6 \cdot 10^{-7}/a$ with a subjective probability of 0.95.

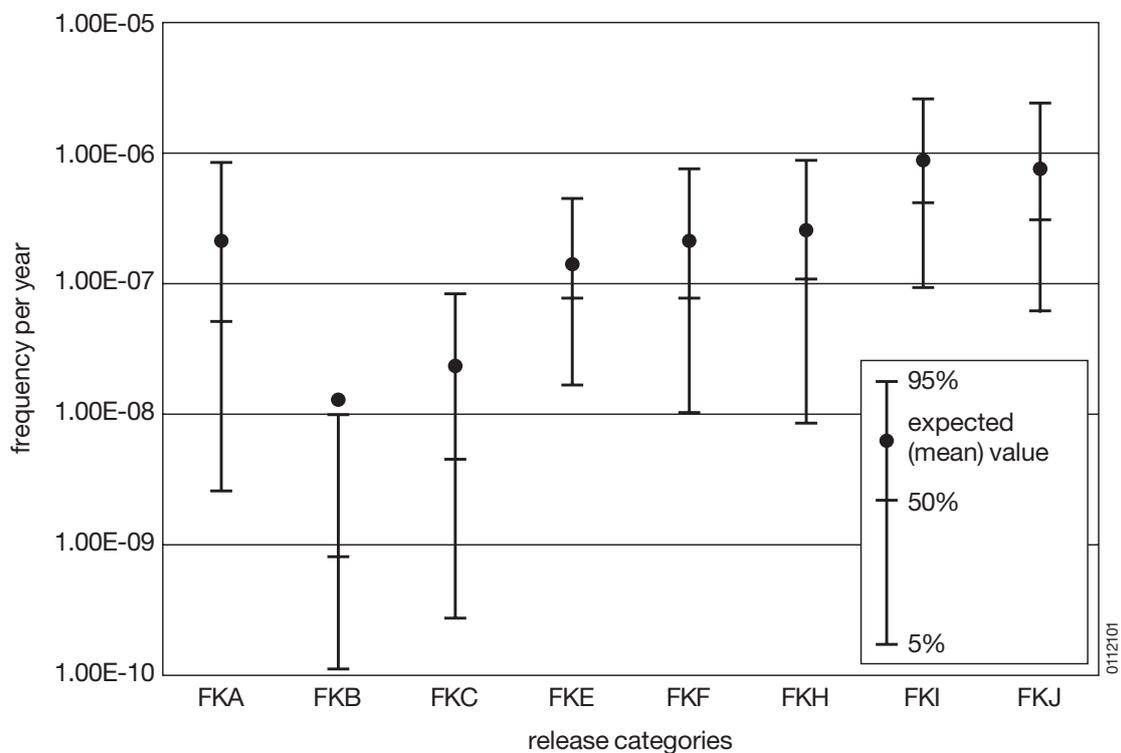


Fig. 6.9 Subjective probability distributions for the expected frequencies of the release categories

For the release categories FKJ and FKI, the quantiles of the subjective probability distribution for the expected frequencies are higher than for all other categories. This favorable statement is somewhat limited by the fact that significant subjective frequencies are calculated for the category FKA (very high releases). When very high quantiles of the subjective probability distribution are considered, the frequency of FKA turns out to be the third highest of all categories. If one compares the quantiles of the subjective probability distributions given in table 6.11 for different categories, FKA seems to be the most significant in terms of risk, defined as the product of damage times frequency.

The uncertainty analysis is linked to a sensitivity analysis. This allows finding out the main reasons for the uncertainties of results. The sensitivity analysis was restricted to the level 2 part. Therefore the relative contribution of uncertainties from level 1 cannot be determined.

The main reason for the significant uncertainty of the expected frequency for release category FKA turned out to be the epistemic uncertainty about the temperature of the main coolant line. This temperature determines the probability of the failure of the coolant line and thus of the pressure relief before RPV failure.

Releases FKB and FKC have a very high subjective probability of a very low expected frequency. High frequencies for FKB are calculated with a very low subjective probability and they are mostly linked to the hydrogen generation rate inside the RPV. This causes detonations in very rare sequences which do not challenge the containment directly by high pressures, but indirectly by mechanical impact at its penetrations.

The expected frequency for category FKE is below $0.45 \cdot 10^{-6}/a$ with a high subjective probability (0.95). The major contribution to its subjective uncertainty range is the uncertainty about the failure probability of the sump suction pipes under core melt impact and the failure rate of filtered containment venting.

For FKE, no dominant contributions to the uncertainty of its expected frequency could be found.

The subjective probability distribution of the expected frequency for release category FKH expresses considerable uncertainty. The most important contributions to this uncertainty are related to the evaluation of ignition sources inside the exhaust ventilation ducts during the filtered venting of the containment.

The expected frequencies for release categories FK1 and FK2 show trends which are contrary to those of the other releases. If a chance combination of uncertain input data results in a low frequency for the other releases, then the frequencies for FK1 and FK2 inevitably must be higher and vice versa. Therefore the major contributions to the uncertainty of the frequencies for FK1 and FK2 are similar to those for the other release categories, but they have an opposite influence.

6.8 Findings related to PSA methods and to plant performance

6.8.1 PSA methods

The present study, which deals with the probabilistic analysis of core melt accidents starting with core damage states and ending with the evaluation of release categories, has evaluated the event tree method applied in Germany for plant specific analyses for the first time. This method allows the consistent representation of very complex relationships, the consideration of uncertain data and assumptions, and the treatment of numerous possible core damage states and branching points within one single mathematical concept. This makes it possible to gain insights which exceed those attained by deterministic analyses. In particular, the identification of sensitive dependencies and uncertainties can be realized with this method by means of Monte Carlo simulations. The almost complete representation of the entire event progression including human actions, which still remains far from being feasible for deterministic methods, contributes significantly to this achievement.

The event tree basically applies a discrete representation of the accident progression. Constant values, such as pressure or time, have to be binned into categories, for example into high, medium and low pressure. This causes an inherent weakness of the method, if some values are near the edge of a category. Further, repeated processes, like the repeated switching on and off of a system, can hardly be represented. To avoid these shortcomings, GRS undertakes methodological developments, which combine stochastic variability of uncertain parameters with deterministic computer codes. This development is not yet ready for application. Furthermore, it will be restricted to single aspects of the event progression for a long time. Therefore event tree analyses will remain necessary in the foreseeable future.

The consistent coupling of the plant damage states - which have been determined by a fault tree analysis - with the event tree analysis of the accident progression makes it possible to trace back particularly significant results, such as the frequency of high releases, to their basic causes on the level of system failures. This allows identifying weak points in the plant.

6.8.2 Plant performance

In about 32 % of all core damage states, coolant injection into the reactor coolant loop starts early enough to keep the core material in the core area or in the lower plenum of the RPV. An injection is possible if the emergency core cooling systems cannot work at the core damage state because of high primary pressure and if later a leak in the primary loop develops, leading to a pressure relief. This sequence is characteristic of a small loss-of-coolant accident or of transients with electric power supply available. In most of the other sequences there is no injection, so that failure of the RPV bottom due to core melt impact cannot be prevented.

If there is high pressure, a pressure relief can take place shortly before RPV failure by way of action of the operating crew, due to leaks in a hot coolant line, or due to stuck-open valves. These three pressure relief mechanisms are taken into account in the event tree. It turns out that in about 90 % of all cases with high pressure in the core damage state there will be a pressure relief before RPV failure. The major contribution comes from the failure of the hot main coolant line.

When the RPV bottom fails at high pressure (3.9 % of all core damage states, including sequences with low and medium pressure upon core damage and with pressure increase during core degradation), consequential damage of the containment has to be assumed. This incident has such severe consequences that future analyses should further increase the degree of confidence for the knowledge about pressure relief mechanisms.

When melt is ejected from the RPV bottom at medium pressure, there is a very low probability (0.6 % of all core damage states) of a subsequent containment failure due to the resulting pressure rise.

A high release of radionuclides is predicted for sequences with bypass of the containment through a steam generator tube leak in about 7 % of all core damage states.

Presently there are only few analyses available for this sequence. As it is rather significant, further investigations are necessary.

Steam explosion, hydrogen combustion and long-term pressure rise are well known threats to the containment which have been analyzed with much effort for a considerable period. No containment failure due to a steam explosion occurred in the event tree analysis although a broad uncertainty range has been assigned to the pertinent input parameters. Due to the effect of the autocatalytic hydrogen recombiners and due to filtered containment venting, the other remaining two phenomena contribute little to the containment failure probability as well. The major contributor for this group of containment failure modes is the failure of containment venting in about 3 % of all core damage states.

During the investigations, another containment threat was identified which consists of the failure of sump suction pipes under core material impact. This incident would open a leak from the inside of the containment to the annulus (about 5.5 % of all core damage states). There is a lack of pertinent analysis in this field. Therefore this estimate is based on assessments of the behaviour of core materials and of the failure margins of the sump suction pipes which are very uncertain.

When the filtered containment venting system is operated, hydrogen-rich gas from the containment will reach the exhaust ventilation ducts on the roof of the auxiliary building. Combustions and consequential damage result in leakages at the ducts in about 10 % of all core damage states. This leads to atmospheric releases at roof height instead of stack height. There are 1.5 % more where the filter of the venting system will be damaged, causing releases without filter function. All assumptions related to these processes are very uncertain. Filtered venting as intended by design without any further damage at the venting system has been calculated for 34 % of all core damage states.

After the failure of the RPV bottom (in 68 % of all core damage states) there will be an erosion of the concrete foundation by the core melt. No convincing arguments could be found for an eventual end of this process, not even when the melt is covered by water. Therefore a complete penetration of the foundation and a contamination of the ground have to be assumed for these sequences.

No further threats to the containment beyond those mentioned above have been identified.

6 Level 2 PSA for normal power operation

The behaviour and the release of radionuclides have been estimated for all failure modes of the containment. Thereby the release path of the radionuclides through the annulus and the ventilation systems located there has been assessed. The releases have been binned into 8 release categories. In general, the quantity of the radionuclides released can be estimated but with a high degree of uncertainty.

Concluding summary:

All frequencies given below in this concluding summary are expected frequencies (mean values) of the distributions calculated by the event tree analysis.

In about 32 % of all core damage states (frequency about $8 \cdot 10^{-7}/a$) the core material will be retained inside the RPV. There will be only small releases through the filtered emergency ventilation system. The major contribution to these sequences comes from core damage states at high pressure and with temperature-induced failure of the main coolant line. This leads to a pressure relief and to a start of the RPV cooling water injection systems.

44 % of all core damage states (about $11 \cdot 10^{-7}/a$) have a limited release through the filters of the containment venting system. This kind of release has to be expected when the RPV bottom fails due to core melt impact, and if there are no additional phenomena which significantly load the containment or the filter of the venting system.

In 1.5 % of all core damage states (about $0.3 \cdot 10^{-7}/a$) the containment venting filter will be damaged by hydrogen combustion, leading to a late unfiltered release. The containment itself remains intact in these sequences. There are sequences with a comparable radionuclide release when the leak control at the containment penetrations fails and unfiltered releases go through the annulus into the environment. This is the case for 7 % of all core damage states (about $1.7 \cdot 10^{-7}/a$).

In 6 % of all core damage states (about $1.5 \cdot 10^{-7}/a$) the containment fails late at overpressure due to a failure of containment venting or due to the melt-through of a sump suction pipe. The release is directed from the containment through the annulus and then through the ducts of the operational annulus venting system without filter.

In 0.5 % of all core damage states (about $0.1 \cdot 10^{-7}/a$) there is an early unfiltered release because the isolation of the containment fails or because hydrogen combustion causes a containment leak.

In 5 % of all core damage states (about $1.3 \cdot 10^{-7}/a$) there is a high release through the secondary system due to a steam generator tube leak. The investigations of the course of events and of the radionuclide release should be continued for this initiating event.

There is high pressure at the failure of the RPV bottom in 3.9 % (about $1 \cdot 10^{-7}/a$) of all core damage states. This results in consequential damage to the containment and a very high release. Main contributions come from sequences with small leak in the reactor coolant loop (including steam generator tube leaks), where the RPV pressure rises significantly shortly before RPV failure due to core melt relocation into the water of the lower plenum. Further contributions are due to sequences with high pressure in the core damage state without pressure relief, neither by active nor by passive mechanisms.

In all sequences with RPV failure, the core melt will continuously erode the concrete foundation, finally reaching the ground below.

7 Level-1 PSA for low-power and shutdown operation

7.1 Introduction

The Basis-PSA (see section 4.3) did not contain analyses for initiating events during low-power and shutdown operation. The available methods for the performance of a PSA for power operation were transferred as far as possible to the low-power and shutdown states for the assessment of the latter and were supplemented by specific approaches, where necessary.

The necessary additions concerned in particular

- the determination of plant operational states during low-power and shutdown operation exemplary with an outage for refueling (see Chapter 7.2),
- the determination of initiating and triggering events and their occurrence probabilities (see Chapter 7.3),
- the adaptation of data concerning common-cause failures (CCF) to the conditions of the low-power and shutdown operation (see Chapter 7.4.1),
- the analysis and assessment of operator actions, as far as they are performed on the basis of experiences from operational practice (see Chapter 7.4.1),
- the determination of time-dependent unavailabilities of system functions during outage (see Chapter 7.4.2 to 7.4.9).

The low-power and shutdown operation comprises the shut down of the plant, the shutdown state and the restart until reaching operation with constant load. Purpose of a planned shutdown from undisturbed specified normal operation may be the performance of repairs, the outage for inspection including refueling or – in case of a longer lasting shutdown – the backfitting of the plant. An unscheduled shutdown may be required in case of malfunctions and incidents. In these cases, in general, a reactor scram will be performed automatically or manually.

During low-power and shutdown operation, different plant operational states are passed through, during which the physical and systems-related state of the plant may change essentially. Examples are:

- Changes of the physical state
 - pressure, temperature and filling level of the primary and secondary system

7 Level-1 PSA for low-power and shutdown operation

- open or closed state of the reactor pressure vessel (RPV)
- Changes of the systems-related state:
 - mode of operation and availability of operational systems
 - availability of the safety systems
 - number of the effective radionuclide barriers

The present PSA on low-power and shutdown states analyzes internal initiating and triggering events (see Chapter 7.3). Internal and external area events have not been included in the analyses, since this would have increased the efforts involved considerably. However, it cannot be excluded that such events deliver a considerably risk contribution. Likewise, possible effects of a failure-induced boron dilution of the coolant on the criticality behavior of the reactor core have not been considered, since it has not been feasible by now to simulate these processes by means of calculations in a substantiated way.

Repair measures and measures of preventive accident management are not included in the analysis. So far, there are no proven methods available for the consideration of these measures or for a level-2 PSA for low-power and shutdown operation.

7.2 Plant operational states

The present analysis refers to an outage with refueling. The low-power and shutdown operation begins with the insertion of the control rods during specified normal operation with the aim of nuclear shutdown of the plant. The low-power and shutdown operation ends when a constant power operation is reached after restart.

At the reference plant, four different types of outage are pre-planned:

- a 7-day short outage with fuel-element shuffling
- a 14-day standard outage

- a 21-day outage with extensive valve inspections
- a 28-day outage with RPV pressure test

The present analysis has been based on the 14-day standard scheduled maintenance inspection by the example of the outage in 1995. All plant operational states passed through during this outage also occur during the other outage types. Actions and measures only occurring in the other outage types have not been considered.

For the description of the changing systems-related and physical states, the outage sequence is subdivided for the analyses in the PSA into plant operational states. The plant operational states are chosen in a way that the systems-related state of the plant within a phase is as constant as possible, whereas the physical state may change within a phase.

Therefore, the analyzed 14-day outage was subdivided in a way that no changes occur, if possible, in the mode of operation and in the extent of the deactivations. Under this boundary condition, 13 plant operational states were defined. They are characterized in Table 7.1 by their essential systems-related and physical features. This classification is plant-specific and cannot be applied to other plants offhand. The term “ $\frac{3}{4}$ -loop-operation” used in Table 7.1 is to be understood as the operating mode during which the coolant level is lowered to three quarters of the diameter of the reactor coolant line. This operating mode is also referred to as “mid-loop operation”.

7.3 Initiating events

As for the PSA for power operation, initiating events are identified first. Regarding the low-power and shutdown operation, distinction has to be made between two categories of initiating events:

1. Events where the system functions for fuel element cooling are not available to the required extent.
2. Events by which larger quantities of unborated water are generated in, or injected into, the primary system.

Table 7.1 Plant operational states of a 14-day standard outage of the reference plant

Identification	Changes of the physical states / System-related features
(1) A0	Power reduction to the condition subcritical hot / Reactor protection signals and availability of the safety systems as during power operation
(1) A1	Shutdown via the steam generators down to primary system pressure 3.1 MPa and primary system temperature 120 °C / All reactor protection systems continue to be available
(1) B1	Primary system cooldown to the condition depressurized cold / Start-up of the residual-heat removal (RHR) system at 120 °C; accumulators and high-pressure pumps are disconnected
(1) B2	Level lowering to mid-loop, mid-loop operation / Core within the RPV, primary system closed pressure-tight
(1) C	Opening the RPV, mid-loop operation / Core within the RPV, primary system not closed pressure-tight, refueling slot gate between settling pond and fuel pool closed
(1) D	Flooding of the reactor cavity, unloading of the fuel elements / Core wholly or in part within the RPV, refueling slot gate between settling pond and fuel pool open
E	Emptying of reactor cavity and RPV / Core fully unloaded, refueling slot gate between settling pond and fuel pool closed, work performed at lower-edge loop
(2) D	Refilling of the reactor cavity, loading of the fuel elements / Core wholly or in part within the RPV, refueling slot gate between settling pond and fuel pool open
(2) C	Level lowering to mid-loop, closing of the RPV / Core within the RPV, primary system not closed pressure-tight, refueling slot gate between settling pond and fuel pool closed
(2) B2	Evacuation and refilling of the primary system / Core within the RPV, primary system closed pressure-tight
(2) B1	Primary system heat-up with the main coolant pumps / All reactor protection signals are available
(2) A1	Deborating of the coolant and taking the reactor to critical condition / Withdrawal of control rods or / and boron dilution
(2) A0	Power increase up to specified level / Reactor protection signals and availability of the safety systems as during power operation

- (1) plant operational states during shutdown
- (2) plant operational states during restart

For the cooling of the fuel elements, the design includes certain operational functions in the different plant operational states. With regard to the first category of initiating events, these operational functions fail or are not available to the required extent. In order to control these initiating events, the failed operational functions have either to be restored or other operational and/or safety functions have to be used. The system functions used to cope with initiating events can be activated automatically or manually by the personnel. Since, in general, there is ample time during low-power and shutdown operation for measures to control initiating events, most of the system functions are activated manually.

The design includes technical and administrative measures to prevent failure-induced injection of larger quantities of unborated water into the primary system. If these measures fail, in a second category of initiating events, larger quantities of unborated water are injected into the primary system which may endanger the subcriticality of the reactor. Moreover, large amounts of unborated water can be generated at the cold leg of the primary side during mid-loop operation in case of loss of primary-side residual-heat removal due to condensation of primary coolant evaporating in the core. This is due to occurrence of a counter-current flow limitation at the entrance of the steam-generator tubes and stagnation of the natural circulation. If the unborated water enters the reactor pressure vessel without mixing, the reactor core could be destroyed by a reactivity excursion. However, there are no corroborated analyses by now on the mixing of a unborated-water plug with the borated coolant and on the possible effects on the reactor core. For the determination of initiating events, the following sources were referred to:

- Operating experience with the reference plant during low-power and shutdown operation,
- reportable events of comparable German plants,
- international operating experience,
- findings from PSAs for low-power and shutdown operation for foreign plants.

Table 7.2 Initiating events during low-power and shutdown operation

Initiating event		Identification
Event group		
Event group		
Transient		
Loss of preferred power-external		T1.1
Loss of preferred power-internal		T1.2
Loss of main feedwater without loss of main heat sink		T2
Loss of main heat sink without loss of main feedwater		T3
Loss of main feedwater and loss of main heat sink		T4
Main-steam leak outside containment		T5.1
Main-steam leak inside containment		T5.2
Feedwater line leak in turbine building		T6.1
Feedwater line leak inside containment; non-isolable		T6.2
Failure of residual-heat removal due to		T7
faulty level lowering		T7.1
failure of residual-heat removal chains		T7.2
unintended activation of the emergency cooling signals		T8
Coolant losses		
Small primary system leak $A < 25\text{cm}^2$		S1
Small primary system leak $25\text{cm}^2 < A < 200\text{cm}^2$		S2
Inadvertently open pressurizer safety valve		S3
Medium primary system leak $200\text{cm}^2 < A < 500\text{cm}^2$		S4
Large primary system leak $A > 500\text{cm}^2$		S5
Inadvertently open pressurizer relief valve due to maintenance fault		S6
Inadvertently open pressurizer relief valve on loss of preferred power		S6/T1
Inadvertently open pressurizer relief valve after turbine trip		S6/T2
Steam-generator tube leak		S7
Leak in the RHR system inside containment		S8.1
Leak in the RHR system in the annulus		S8.2
Leak in the volume control system		S9
Leak in the reactor cavity / setdown pool		S10
Leak into an affiliated system		S11
Boron dilutions		
Leaks from deborated-water-carrying systems		D1
Steam-generator tube leak		D1.1
Leak in the RHR heat exchanger		D1.2
Leak in a bearing seal		D1.3
Inadvertent primary system injection		D1.4
Inadvertent presence of unborated water in the RHR system		D2
Boron dilution during decontamination work		D3
Boron dilution during level raising		D4
Borating fault on shutdown		D5
Inadvertent boron dilution on shutdown following loss of all main coolant pumps		D6/T1
Criticality events		
Inadvertent control rod withdrawal		K1
Loss of reactor scram		K2

■ initiating events for which occurrence probability was determined

1) RHR residual heat removal-

see Table 7.1

Plant operational states ¹⁾													
Shutdown				E					Restart				
A0	A1	B1	B2	C	D	E	D	C	B2	B1	A1	A0	
RPV closed				RPV open					RPV closed				
x	x	X	U	U	x	x	x	x	x	x	x	x	x
					x	x	x						
x	x										x	x	
x	x										x	x	
x	x										x	x	
x	x										x	x	
x	x										x	x	
		x	x	x	x		x	x	x	x			
			U						x				
		x	U	U	x		x	x	x	x			
			U										
x	x	x								x	x	x	
x	x	x								x	x	x	
x	x	x								x	x	x	
x	x	x								x	x	x	
	x	x	x							x	x	x	
x	x	x								x	x	x	
x	x	x								x	x	x	
x	x	x								x	x	x	
		x	U	U	x	x	x	x	x	x			
		x	U	U	x	x	x	x	x	x			
x	x	x	x	x	x	x	x	x	x	x	x	x	x
					x			x					
		x	x	x	x	x	x	x	x	x			
		x	x	x	x	x	x	x	x	x			
		x	x	x	x	x	x	x	x	x			
		x	x	x	x	x	x	x	x	x			
									x				
										x			
	x											x	
													x
										x	x		
x													X

■ plant operational states with high relevance for the respective initiating event

U initiating event being analysed up to system damage states
 x the initiating event can occur in this plant operational state

7 Level-1 PSA for low-power and shutdown operation

The initiating events were assigned to those operation states in which they can occur. This classification leads to a spectrum of initiating events which can be seen in Table 7.2. The initiating events are subdivided into four groups. For the first two groups, the transients and coolant losses, the system functions for fuel element cooling are no longer available. Regarding the third group, i.e. the boron dilutions, the system functions for avoiding the injection of unborated water into the primary system failed. Regarding the fourth group, the criticality events, the fuel element cooling is no longer ensured, because shutdown systems fail and consequently the reactor power cannot be reduced.

Contrary to the power operation, the group of transients during low-power and shutdown operation is subdivided into loss of preferred power-external and loss of preferred power-internal. The loss of preferred power, which corresponds to the loss of the auxiliary power supply, can be caused by external triggering events (e.g. lightning, loss of offsite power) or by internal triggering events (faulty connections during maintenance work). Losses of preferred power due to faulty connections in general cannot occur, contrary to loss of preferred power-external, in all plant operational states and their occurrence probability is not time-dependent. For this reason, the two cases are dealt with separately.

The second column of Table 7.2 shows abbreviated references to the respective initiating event. Initiating events, for which the probabilities per outage were determined (see Chapter 7.3.1), are shaded pink. The other columns of Table 7.2 indicate the plant operational states according to their identification in Table 7.1. Initiating events which can occur in a specific plant operational state are indicated in the corresponding column with an (x) or a (U). Initiating events indicated with a (U) have been examined for the corresponding plant operational state with event tree and fault tree analyses. In case of initiating events which can occur in more than one plant operational state, the plant operational states with the highest relevance are shaded gray. In cases where more than one operating state is shaded gray, the plant operational state with the highest relevance can only be determined after further analyses.

For the initiating events, occurrence probabilities during outage or during a plant operational state are determined. The determined probabilities for the initiating events examined more detailed in the present PSA, are dealt with in Chapter 7.3.1. These events are compiled in Table 7.3. They are identical with the initiating events shaded pink in

Table 7.2. The determined probabilities for initiating events not examined more closely in the PSA, are discussed in Chapter 7.3.2.

Initiating events whose probabilities can be directly determined on the basis of the operating experience, are indicated in Table 7.3 with “OE”. If an initiating events did never occur, the estimate value of the probability is exclusively determined by the observation basis (period or number of the outages). Due to the relatively small observation basis, a considerable overestimation of the actual probability can occur. In order to achieve realistic estimates in such cases, the initiating event (e.g. loss of residual-heat removal due to faulty level lowering) is put down to triggering events whose probabilities can be determined on the basis of operating experience (e.g. inadvertently open valve) The initiating events which are put down to triggering events are indicated in Table 7.3 with “FT”.

The initiating events shaded yellow in Table 7.3 are further examined by means of event tree and fault tree analyses.

7.3.1 Analyzed initiating events and their probabilities

Only those initiating events were analyzed more detailed in the PSA which are typical for low-power and shutdown operation and which are expected to deliver essential contributions to the probability of system damage states.

- **Determination of probabilities**

The probabilities determined from operating experience are based on the evaluation of operating experience with pressurized water reactors in Germany for shutdown and restart as well as on outages in the period from 1986 to 1996. In cases where the observation period for the initiating events was too short (e.g. for leaks) the world-wide experience with PWR plants was referred to in addition.

Table 7.3 Probabilities for initiating events (mean values) during the 14-day standard outage

Initiation event				
Event group	Identification			
	Event	POS	p	PD
Transients				
Loss of pref.power-extern. (20 h mid-loop-op.)	T1.1	1B2, 1C	4.8E-4	OE
Loss of preferred power-internal	T1.2	D,E	2.5E-2	OE
Loss of MHS without loss of MFW	T3	1A1	6.6E-3	OE
Loss of MFW with loss of MHS	T4	1A1	3.9E-3	OE
Loss of residual-heat removal due to	T7			
faulty level lowering	T7.1	1C	4.9E-6	FT
failure of RHR chains	T7.2	1B2, 1C	4.8E-5	FT
unintended activation of the ECCS signals ¹⁾	T8	1B2	7.6E-3	OE
Coolant losses				
Inadvert. open P-RV due to maintenance fault	S6	1A1	6.7E-3	OE
Steam-generator tube leak < 2 F	S7	1B1	5.0E-4	OE
Leak in the RHR < 25 cm ²	S8		5.0E-4	OE
S8 inside containment, RPV closed	S8.1	1B2, 1C	1.25E-4	
S8 inside annulus, RPV closed	S8.2	1B2, 1C	1.25E-4	
Leak in volume control system < 25 cm ²	S9	1B1	5.0E-5	OE
Leak in the reactor cavity/setdown pool	S10	1D	4.0E-5	FT
Leak in an affiliated system	S11	1B2,1C	<1.0E-7	FT
Boron dilution				
Leaks from unborated-water-cont. systems	D1			
Steam-generator tube leak	D1.1	1B2,1C	5.0E-4	OE
Leak in the RHR heat exchanger	D1.2	1B2,1C	5.0E-4	OE
Leak in a bearing seal	D1.3	1B2,1C	9.5E-3	OE
Inadvert. primary-system injection via P-relief tank/pressurizer	D1.4	1B2	4.6E-6	FT
Borating fault on shutdown	D5	1A1	2.3E-4	FT
Inadvertent boron dilution on shutdown following loss of all main coolant pumps	D6/T1	2A1	3.0E-8	FT

	system damage states-	initiating events analyzed up to Ppressurizer
1)	probability without decoupling of the reactor protection 3,6E-2	FT fault-tree analysis
RV	relief valve	MFW main feedwater
OE	operating experience	MHS main heat sink
		p probability
		RPV reactor pressure vessel
		PD probability determination

Regarding the determination of the probability of an event on the basis of operating experience, distinction is made between initiating events depending on the duration of the plant operational states and initiating events depending on certain actions. If the event is time-dependent, the observed events are referred to the cumulated times of the evaluated operating experience. The probabilities for the occurrence of the event within a plant operational state is then determined on the basis of the duration of the plant operational state. An example is the “loss of main heat sink without loss of main feedwater”, which can occur at any time within the plant operational states during shut-down and restart.

Event which can occur to certain actions, thus being independent of the duration of a plant operational state, are referred to the number of the evaluated plant operational states in which they can occur. An example is the “loss of residual heat removal by unintended activation of the emergency core cooling signals”, which can only occur at a specific point in time during level lowering below the pressurizer water level of 2.28 m. For this initiating event it was taken into consideration that in nine of eleven outages at the reference plant the reactor protection was decoupled in the relevant plant operational state and thus the event could not occur during these outages.

Regarding the probabilities for leakages, the different boundary conditions are to be considered in dependence on the leak location and the point of time when the leak occurred. A leak in the RHR train (S8) during mid-loop operation can either occur inside the containment (S8.1) or inside the annulus (S8.2), with the reactor pressure vessel being closed (plant operational state 1B2) or open (plant operational state 1C). The probability was attributed accordingly in equal shares.

As for those initiating events which were not observed during plant operation, the triggering events that can lead to an initiator and for which reliability data are available from operating experience were determined by fault tree analysis (indicated in Table 7.3 with “FT”). Contrary to power operation, a large number of combinations of triggering events is analyzed here, which in addition can influence the system functions challenged to control the event. In these cases it is necessary to include the fault tree of the triggering event into the overall fault tree for the determination of the system damage states. The probabilities for initiating events determined this way reflect the systems engineering of the reference plant.

7 Level-1 PSA for low-power and shutdown operation

For those initiating events which were put down to triggering events, Table 7.4 presents the probabilities of the dominant initiators, the associated conditional probabilities for the failure of counter measures under the condition that there was a triggering event, and the total of the probabilities of the initiating events. In the following, the triggering events are described:

- The “failure of residual-heat removal due to faulty level lowering (T7.1)” can be caused by a failure of the mid-loop measuring system in upward direction OR failed closure of the LP reducing station AND the failure of automatic deactivation AND the failure of manual deactivation by the operating personnel. The dominant initiators in Table 7.4 are the first four failure combinations of the fault-tree evaluation.
- The “failure of residual-heat removal due to failure of the residual-heat removal chains (T7.2)” is caused by the failure of all operational RHR chains due to CCF or CCF in combination with independent failures. As above, the dominant initiators in Table 7.4 are the first four failure combinations of the fault-tree evaluation.
- In the case of the “leak in the reactor cavity/ setdown pool (S10)”, a crash of a fuel element during transport from the reactor pressure vessel to the fuel pool onto the transition area between the RPV-flange connection and the reactor cavity was postulated. The triggering event was determined on the basis of German operating experience on the transport of fuel elements (zero-faults statistics). The probability of crashes onto the relevant areas considers the relation between the length of the crash area and the transport distance.
- To determine the probability of a “leak into an affiliated system (S11)”, all possibilities of an inadvertent extraction of coolant from the primary system were analyzed. systems connecting to the primary system were systematically analyzed Leakages with a mass flow rate of less than 1 Mg/h or with a probability $< 1.0 \cdot 10^{-7}$ were assessed as negligible. The examination did not reveal any relevant leak possibilities. The values stated in Table 7.4 were determined for the failed closure of the LP reducing station.
- To determine possible injections of unborated water into the primary system from unborated-water-carrying systems, all primary-system connections were systematically analyzed. Due to the injection of the large amounts of unborated water, the “inadvertent primary-system injection via the relief tank/ pressurizer (D1.4)” is the dominating event.

- The boron dilution events "borating fault on shutdown (D5)" and "inadvertent boron dilution on shutdown following loss of all main coolant pumps (D6/T1)" are due to the failure of the injection concentration monitoring system. In the case of the initiating event D6/T1, the loss of preferred power during boron dilution for restart initiates the failure of all main coolant pumps.

- **Analyzed initiating events**

The initiating events analyzed in the PSA for low-power and shutdown operation in detail are shaded yellow in Table 7.3. The second column of Table 7.3 includes, in addition to the abbreviated references to the initiating events, the respective relevant plant operational state. The analyzed events either cause a failure of the residual-heat removal via the RHR-chains in case of mid-loop operation or a boron dilution.

The transients and coolant losses are analyzed in the plant operational states 1B2 and 1C during shutdown, since in these phases the level is lowered to three quarters of the diameter of the main coolant line ($\frac{3}{4}$ -loop operation or mid-loop operation) and the decay heat generation is still relatively high. The minimum requirements regarding the system functions for the control of the initiating events are therefore more stringent in these plant operational states than during mid-loop operation before restart. At this time, the decay heat generation is about 24 MW. In the outage under review, the mid-loop operation lasts for about 20 h at closed primary system and another 20 h at open primary system.

Regarding the initiating events with boron dilution of the primary system, the analyses are limited to those system functions by means of which an injection into the primary system is prevented. Corroborated analyses on the mixing of the unborated water and on the reactivity effects during passage through the core cannot be performed with the methods available at present.

Table 7.4 Expected values of the probabilities for triggering events per outage

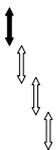
Triggering event		Transition
Description	p	Relevant system function
CCF transducer of the loop measurement 3of4 (2 relevant combinations)	2.8E-6	Depends on the logical combinations of the initiating events (basic events) with the triggering event (TOP-event in fault tree)
CCF transducer of the loop measurement 4of4	8.0E-7	
Failed closure of the LP reducing station	9.6E-7	
Rest	3.4E-7	
CCF operational failure of the RHR pumps 4of4	1.9E-5	Depends on the logical combinations of the initiating events (basic events) with the triggering event (TOP-event in fault tree)
CCF operational failure of the RHR pumps 3of4 (2 relevant combinations)	1.3E-5	
CCF operational failure of the RHR pumps 2of4	4.3E-6	
Rest	1.2E-5	
Crash of a fuel element per transport	4.0E-3	Crash onto the seal liner in the transition area between RPV and setdown pool
Failed closure of HP reducing station (automatically or manually) and failure of position monitoring	2.7E-5	Operator does not close HP reducing station and gate valve behind HP reducing station fails to close
Loss of volume control system of relief tank and loss of filling-level indication	2.3E-3	Loss of further indications
Failure of the injection concentration monitoring	2.3E-4	Depends on the logical combinations...(see T7.1, 1C)
Loss of pref.power during boron dilatation for restart	1.3E-4	Failure of the injection concentration monitoring

1) dominant contribution to CCF
 CCF common-cause failures
 HP high pressure

LP low pressure
 p probability
 RPV reactor pressure vessel

events and for the transition of triggering events to initiating events

probability p	Initiating Event		Identification
	Description	p	
	Failure of residual-heat removal due to faulty level lowering	4.9E-6	T7.1, 1C
	Failure of residual-heat removal due to failure of operational RHR chains	4.8E-5	T7.2 1B2 or 1C
1.0E-2	Leak in the reactor cavity / setdown pool	4.0E-5	S10, 1D
3.7E-3	Leak via HP reducing station	1.0E-7	S11, 1B2 ¹⁾
2.0E-3	Inadvertent primary-system injection via relief tank / pressurizer	4.6E-6	D1.4, 1B2
	Borating fault on shutdown	2.3E-4	D5, 1A1
2.3E-4	Inadvertent boron dilution on shutdown following loss of all main coolant pumps	3.0E-8	D6/T1, 2A1



7.3.2 Estimates on events not or not completely analyzed events

For the events not further analyzed from Table 7.2, distinction has to be made regarding the following cases:

- Initiating events for which occurrence probability was determined, but no event sequence analysis was performed (see Chapter 7.3.2.1),
- initiating events which were only analyzed in selected plant operational states (see Chapter 7.3.2.2),
- initiating events for which no probabilities were determined and no analyses were performed (see Chapter 7.3.2.3),
- injection of unborated water into the primary system, for which possible causes were investigated, but no complete analysis (up to a system damage state) was performed (see Chapter 7.3.2.4).

7.3.2.1 Events whose probabilities were determined

These events are stated in Table 7.3, but not shaded yellow. The probability for these events was determined

- on the basis of operating experience,
- on the basis of the PSA for power operation, or
- on the basis of analyses of triggering events.

- **Loss of preferred power-internal**

The probability for a “loss of preferred power – internal” was determined on the basis of operating experience. The losses of preferred power observed were initiated by (internal) deactivation faults during limited grid connection of the plant. This event only occurs in plant operational states where the reactor cavity is filled and thus a very long grace time is available for the control of the event. Potential problems regarding restoration of grid supply due to a limited grid supply have not been analyzed.

- **Loss of main-heat sink without loss of main feedwater**

The “losses of main-heat sink without loss of main feedwater” were observed on the basis of operating experience during shutdown and restart. Thereupon, the events

were analyzed to whether they could have occurred both during shutdown and restart. However, the initiators of the events during restart were restart-specific (fault due to maintenance work) and were not possible to occur during shutdown. Therefore, the further examination was performed separately for shutdown and restart each. It showed that the events during restart are negligible compared to the events during shutdown. This is due to the low decay heat generation and the resulting long grace times, and the low requirements regarding the system functions. Thus, the analyses only comprise two events which occurred during shutdown. On this basis, a probability of $6.6 \cdot 10^{-3}$ was determined for the initiating event (see Table 7.3). With the non-availability of the system function of $1.9 \cdot 10^{-5}$, determined by the analyses on low-power and shutdown operation, the contribution to system damage states is estimated to be about $1.2 \cdot 10^{-7}$. Thus, the contribution of the event to the overall probability for system damage states is about 5 %. This contribution was not taken into account. For the final assessment, a detailed analysis of the initiating event is required.

- **Loss of main feedwater without loss of main-heat sink**

At the reference plant, a “loss of main feedwater with loss of main-heat sink“ occurred during shutdown. With the non-availability of the system function of $3.9 \cdot 10^{-5}$, determined by the analyses on low-power and shutdown operation, the contribution to system damage states is estimated to be about $1,5 \cdot 10^{-7}$, which corresponds to a contribution to the overall result of about 6 %. The event was not considered in the overall probability for system damage states for the same reasons as for the above “loss of main-heat sink without loss of main feedwater”.

- **Inadvertently open pressurizer relief valve (P-RV) due to maintenance fault**

An “inadvertently open P-RV due to maintenance fault” was observed two times at the reference plant. In one case, the relief valve opened temporarily due to faulty wiring during low-pressure restart. In the second case, it opened due to a maintenance fault at subcritical hot condition. The two events differ that significantly regarding the requirements for the system functions that they have to be analyzed separately. The first event can only occur with low restart pressure and is neglected due to the low requirements for the system functions. The second event leads to a leak at the pressurizer if the shut-off valve fails (non-availability $6.4 \cdot 10^{-3}$ at tests with three-months intervals). With a probability of $3.4 \cdot 10^{-3}$ (for one event), there is a probability of about $2 \cdot 10^{-5}$ for a

leak at the pressurizer. For the PSA for low-power and shutdown operation, this leak was neglected in comparison to the more probable “leak due to inadvertently open safety valve”. With the non-availability of the system functions of $4.8 \cdot 10^{-4}$ for this leak, the contribution to system damage states is estimated to be about $1 \cdot 10^{-8}$. This corresponds to a contribution to the overall result of less than 1 %. For this reason, the initiating event was neglected.

- **Steam-generator tube leak**

The probability for a “steam-generator tube leak” was derived from the probability for such a leak during power operation. Here, the specific loads during shutdown and the world-wide operating experience, as far as transferable, were taken into account.

The probability for a “steam-generator tube leak” during shutdown of the plant was determined at $5 \cdot 10^{-4}$. The analyses on “steam-generator tube leak” during power operation revealed a non-availability of the system functions of $8.5 \cdot 10^{-5}$. If this non-availability is also applied to low-power and shutdown operation, a contribution to system damage states of about $4 \cdot 10^{-8}$ is achieved. This value corresponds to about 1 % of the overall probability for system damage states. Therefore, the initiating event was not analyzed more detailed. Further, there were no analyses on how far the control becomes more difficult if the leak can no longer be detected by means of the N16 detection.

- **Leak in the volume control system**

The probability for a “leak in the volume control system” was likewise derived from the probability for such a leak during power operation.

Event sequences due to a “leak in the volume control system” in the non-isolable area of the RHR system develop as the analyzed leak in the RHR system in the annulus. Thus, the non-availability of the system functions for a leak in the RHR system of $2.2 \cdot 10^{-4}$ can be referred to for estimating the contribution to the probability of system damage states. With the probability of $5 \cdot 10^{-5}$ for the leak, there is a probability of about $1 \cdot 10^{-8}$ for system damage states due to the leak. Thus, the contribution is about 1 % and will therefore be neglected. For a leak location in an area of the volume control system, which can be isolated against the RHR system, the contributions to the system

damage states are estimated to be even smaller due to the lower non-availability of the system functions.

- **Leak in the reactor cavity/setdown pool**

As cause of a “leak in the reactor cavity/setdown pool”, the crash of a fuel element onto the transition area between reactor pressure vessel and setdown pool was analyzed. The probability of the leak was calculated at $4 \cdot 10^{-5}$. From the leak, the coolant would flow into the area below the RPV and via connecting lines into the containment sump until the reactor cavity is emptied in case of overfeeding the leak. The core remains covered with coolant. The initiating event was classified as negligible, since the residual heat removal from the reactor pressure vessel is not endangered by the leak.

- **Leak in an affiliated system**

For the determination of the probability of a “leak in an affiliated system”, all connections to the primary system were systematically examined regarding component failures or maintenance faults which may lead to this event. It showed that the leak flow rates are either very small or the probability for a leak is $< 1 \cdot 10^{-7}$. Thus, the initiating event was neglected.

7.3.2.2 Events only analyzed in selected plant operational states

The initiating events were analyzed for those plant operational states for which the most stringent minimum requirements for the system functions to control the events have to be applied. However, it was not analyzed whether conditions can occur in the plant operational states analyzed so far, which may impair the control of the event.

7.3.2.3 Events for which no probabilities were determined and no analyses were performed

These events primarily concern transients and coolant losses analyzed during power operation, but which can also occur in the plant operational states A0 and A1 during shutdown or restart, respectively. Since the reactor protection in these phase is available, as during power operation, it is assumed that these initiating events are covered

by the analyses on power operation regarding their possible sequences. However, it was not analyzed in the PSA whether reactor protection signals are not actuated and thus the preconditions for the control of the event become less favorable compared to power operation.

7.3.2.4 Handling of boron dilution events

In different plant operational states of the low-power and shutdown operations, unplanned boron dilutions of the coolant may occur. One of the potential causes, i.e. the accumulation of nearly boron-free condensate during residual heat removal via a steam generator, was already dealt with in connection with the failure of the residual heat removal. Further, unplanned boron dilutions were analyzed, which may be caused by injection of unborated water into the primary system from outside. However, these analyses only cover the loss of those system functions which prevent the injection of unborated water into the primary system. Possibilities of detection and interruption of the injection of unborated water via primary-side indications have not been analyzed yet. In so far, the analyses have not been finalized and do not deliver system damage states as final states yet. Likewise, substantiated statements on the mixing of the injected unborated water on the way up to the passage through the core and the reactivity effects cannot be made yet. The expected probability for the initiating event leading to the injection of unborated water into the primary system is presented in Tables 7.3 and 7.4. In the following, the analyzed causes for injection of unborated water are described.

- **Injection of unborated water via a steam-generator tube leak (D1.1), plant operational state 1B2, 1C, (mid-loop operation, RPV closed, RPV open)**

The injection of unborated water is initiated by an undetected steam-generator tube leak during shutdown. After reducing the pressure in the primary system to the secondary side pressure via a steam-generator tube leak in the lower region of the steam generator unborated water can enter either the hot leg or the cold leg of the primary circuit. If the leak is in the cold leg unborated water can accumulate in the pump suction line. If the unborated water is accumulated in the hot leg an effective mixing can be assumed, either by the operating decay heat removal system in the respective loop or by the coolant volume in the upper plenum. The mass of unborated water injected depends on the leak mass flow.

- **Injection of unborated water via a leak in the RHR heat exchanger (D1.2), plant operational state 1B2, 1C, (mid-loop operation, RPV closed, RPV open)**

After reducing the pressure in the primary system the pressure in the RHR circuit is lower than in the component cooling system. In this case via a leak in the RHR heat exchanger unborated water could enter the RHR system leg. Unborated water can enter only the RHR system leg in standby, because the pump pressure prevents unborated water to enter the operating leg. If the stand-by leg is switch into operating mode the unborated water would be fed into the primary circuit.

The leak can be detected by water level indicators for the component cooling system. Depending on the status of the fill-up of the component cooling circuit two different event sequences are possible. If the automatic fill-up fails, a transition probability of $4 \cdot 10^{-2}$ has been estimated that the leak is not detected. The unborated water injection in this case has a probability of $2 \cdot 10^{-5}$. If the automatic fill-up is working larger amounts of unborated water will be injected only if both the leak detection and the daily balancing of unborated water injection fail due to operator error. For this case a transition probability of $1.4 \cdot 10^{-4}$ and thus a probability of $7 \cdot 10^{-8}$ for the accumulation of a larger amount of unborated water in the RHR system leg have been estimated.

- **Deionate insertion via a leak in a bearing seal (D1.3), plant operational state 1B2, 1C, (mid-loop operation, RPV closed, RPV open)**

The probability of a leakage of a floating ring shaft seal has been evaluated based on operating experience. Taking into account various possibilities to detect the leak a transition probability of $6.5 \cdot 10^{-4}$ has been evaluated, that unborated water enters the RHR system leg without being detected. This results in a probability of $6.2 \cdot 10^{-6}$ for larger amounts of unborated water to enter the RHR system leg. As for the event D 1.2 it has been assumed, that the leak occurs in the injection leg and that the unborated water enters the primary circuit upon changing the RHR leg to the injection leg.

- **Deionate insertion due to inadvertent primary-system injection (D1.4), plant operational state 1B2, (mid-loop operation, RPV closed)**

The possibilities of an inadvertent injection of unborated water have been investigated and evaluated. The relevant initiating event is the inadvertent injection into the pressur-

izer via the pressurizer relief tank from the unborated water supply system GHC caused by a failure of the level measurement (see Table 7.4). With a probability of $4.6 \cdot 10^{-6}$ an injection of unborated water into the pressurizer occurs and after the dome plate is filled unborated water enters the hot leg via the surge line. It has been estimated that about 180 Mg/h unborated water can be injected. The further course of the event depends on the operation of RHR system leg of the affected cooling circuit. With a probability of $5 \cdot 10^{-1}$ the injected unborated water will be drawn in and mixed via the operated RHR system leg. With the same probability of $5 \cdot 10^{-1}$ unborated water is injected into, and mixed in, the upper plenum. In both cases the unborated water will be homogeneously mixed and critical boron concentrations would result only after long periods of time. Possibilities for detection, e.g. by the water level measurement in the primary circuit, have not yet been investigated.

- **Faulty borating for shutdown (D5), plant operational state 1A1 (shutdown via the steam generators)**

Faulty borating for shutdown can be caused by a failure of the injection concentration control, so that only deionate but no boron is injected. For the injection concentration control an unavailability of $2.3 \cdot 10^{-4}$ has been evaluated. It has been estimated that an amount of about 30 Mg unborated water can be generated.

- **Inadvertent boron dilution on shutdown following loss of all main coolant pumps (D6/T1), plant operational state 2A1, (boron dilution and taking the reactor to critical condition)**

A plug of unborated water can be generated during boron dilution for shutdown, if during this phase both the main coolant pumps and the injection concentration control fail. The main coolant pumps have been assumed to fail due to a loss of preferred power for 5 h. For the injection concentration control an unavailability of $2.3 \cdot 10^{-4}$ has been evaluated. This results in a probability of $3 \cdot 10^{-8}$ for the initiating event (see Table 7.4).

Table 7.5 Mean values of the probabilities per outage of the transition from initiating

No	System damage states			p	Transition probability (Event group, Event- Tran-		
	Identification A	D	K [h]		T1.1, 1B2 4.8E-4	T1.1, 1C 4.8E-4	T7.1, 1C 4.9E-6
Fuel element cooling							
1	<u>P(b1,b3)S</u>	LP	2 - 3	9.6E-8		2.0E-4	
2	<u>P(b1)S</u>	LP	3 - 4	1.4E-6		5.1E-4	
3	<u>P(b3)S</u>	MP	1 - 2	< E-9			< E-9
4	<u>P(b3)S</u>	LP	1 - 2	< E-9			
5	<u>P(b1)S</u>	MP	3 - 6	1.1E-6	9.8 E-5		9.4E-5
6	<u>P(b1)S</u>	HP	5	9.1E-8			
7	<u>P(b4)S</u>	HP	1 - 2	< E-9			
Deboration							
8	<u>P(d)S</u>		4 h	3.5E-8	4.6E-6		2.0E-7

- | | | | |
|----|------------------------------------|----|---------------------------------|
| 1) | see Table 7.3 | d | Deboration after RHR failure |
| A | Failure cause | D | Pressure in the primary circuit |
| b1 | RHR failure | HP | high pressure |
| b3 | loss of feedwater | K | Time window for AM and recovery |
| b4 | overpressure in the primary system | | |

7.4 Transition from initiating events to system damage states

From low-power and shutdown operation the plant can enter a system damage state,

- if the fuel element cooling fails
(after an uncontrolled initiating event of class 1) or
- if larger amounts of unborated water are generated in, or are injected into, the primary circuit (after an uncontrolled initiating event of class 2).

Dependent on initiating event and event sequence system damage states with different characteristics can occur. Which system damage states can occur from low-power and shutdown operation, is evaluated by means of event tree analyses for the initiating events to be investigated.

events to system damage states and of the system damage states

for initiating events ¹ plant operational state, -Identification)						
sients			LOCAs			
T7.2, 1B2	T7.2, 1C	T8, 1B2	S8.1, 1B2	S8.1, 1C	S8.2, 1B2	S8.2, 1C
4.8E-5	4.8E-5	7.6E-3	1.3E-4	1.3E-4	1.3E-4	1.3E-4
5.8E-6						
1.7E-2				1.42E-3	1.42E-3	
< E-9			2.4E-7	2.4E-7		
				5.7E-6	5.7E-6	
2.3E-3	1.2E-4		2.17E-4	2.17E-4		
4		1.2E-5				
		< E-9				
6.5E-4		5.4E-6		5.4E-6		

MP medium pressure
 LP low pressure
 p probability
 P primary side failure
 S secondary side failure



These analyses are described in chapters 7.4.2 to 7.4.9, their results are summarized in Tables 7.5 to 7.7 (and in Figures 7.1 to 7.5). For a better understanding of the event tree analyses the types of system damage states identified by the analyses are characterized already in this place.

The PSA for low-power and shutdown operation distinguishes between eight types of system damage states, of which seven are connected with a failure of the fuel element cooling and one with the formation of unborated water in the primary circuit. For events leading to unborated water injection into the primary circuit no event tree analyses have been performed. Such events are discussed in chapter 7.3.2.4, partly their probabilities are estimated.

The individual system damage states have the following characteristics:

– system damage states affecting the fuel element cooling

- | | | | |
|----|----------------------------------|----|---------|
| 1. | $\underline{P}(b1,b3)S$ | LP | 2 - 3 h |
| 2. | $\underline{P}(b1)S$ | LP | 3 - 4 h |
| 3. | $\underline{P}(b3)S$ | MP | 1 - 2 h |
| 4. | $\underline{P}(b3)S$ | LP | 1 - 2 h |
| 5. | $\underline{P}(b1)\underline{S}$ | MP | 3 - 6 h |
| 6. | $\underline{P}(b1)\underline{S}$ | HP | 5 h |
| 7. | $\underline{P}(b4)\underline{S}$ | HP | 1 - 2 h |

– system damage states of deboration

- | | | | |
|----|----------------------|--|-----|
| 8. | $\underline{P}(d)S,$ | | 4 h |
|----|----------------------|--|-----|

The system damage states are characterized by the following elements:

- Failure of secondary side „S“ or primary side „P“ system functions for heat removal resp. prevention of deboration.
- Primary failure cause, leading to a system damage state: b1 (failure of RHR), b3 (loss of water injection), b4 (overpressure in the primary circuit) und d (deboration after failure of RHR).
- Pressure in the primary circuit (LP = low, MP = medium, HP = high).
- Time window to prevent core damage states.

The system functions to be kept available during the various plant operational states are defined in the operators manual. Thermohydraulic analyses have been performed in order to evaluate the system function success criteria.

Applying the methods of the event tree and fault tree analyses the PSA has evaluated the probabilities, that the provided system functions do not cope with an initiating event and that the event sequence leads to a system damage state. Table 7.5 shows the probabilities (mean values) for the transition from initiating events to system damage states. In Table 7.5 also the probabilities of the system damage states are shown. The probabilities of the individual system damage states result from the sum of the products of the initiating event probabilities and the corresponding transition probabilities.

In table 7.6 for the initiating events the unavailabilities of the required system functions, the main contributions to the unavailabilities and the importances of common cause

failures (CCF) and human errors (HE) are shown. Furthermore the probabilities of system damage states resulting from different initiating events and their total values are shown.

In the following section 7.4.1 the approach to evaluate the component reliability data is described. The sections 7.4.2 to 7.4.9 describe the event tree analyses for the initiating events, which have been investigated in detail.

7.4.1 Reliability data

In order to evaluate the transition probabilities from initiating events to system damage states reliability data for components and operator actions are required. In the following the evaluation of these data for low-power and shutdown operation is described.

- **Independent failures of single components**

The reliability data for independent failures in low-power and shutdown operation generally have been evaluated based on the set of reliability data for power operation. For identical components and identical failure modes the reliability data have been taken from the data set. For similar components reliability data have been derived from the data set for power operation taking into account differences of the kind of component, of operation modes and of maintenance concepts. Examples are:

- „Water level control mid-loop operation does not control “ is similar to „Low power control does not control “,
- „Accumulator check valve does not open in tip-operation “ is similar to „Accumulator check valve does not close resp. open in motor operation “.

Reliability data for components which in power operation are not required to cope with initiating events or whose failure mode is different, have been estimated by a plant specific or, if this was not possible, by a generic evaluation of the operating experience.

This category comprises, e.g.,

- components pertaining to the mid-loop measurement,
- components of the RHR system required in the RHR,
- components of the LP-reduction station

- components of the flow rate control for boric acid and unborated water.

For one component (flow rate control boric acid) up to now no reliability data have been evaluated for the application in nuclear technology. Taking into account the specific requirements in nuclear technology data from chemical process plants could be used in this case, i.e.

- „Flow rate control boric acid, faulty indication of too high value “ is similar to „ph-measurement in chemical process plant, faulty indication of too high value“.

- **Common cause failures**

Also for the evaluation of reliability data for common cause failures (CCF) the data set for power operation has been used as basis. However, additional data have been required mainly for the following components resp. failure modes which did not appear in the PSA for power operation:

- flow rate measurement of the boric acid and deionate injection
- water level measurement during mid-loop operation
- operational failure of the RHR chains during mid-loop operation

For the flow rate measurement of the boric acid and deionate injection the CCF probabilities have been calculated taking into account the monthly staggered test interval of the flow rate measurements. According to a modified test instruction the measuring circuits of the mid-loop measurement are checked no longer than ten days before plant shut down, and the pressure sensing lines are rinsed shortly before lowering the water level at an already reduced primary circuit pressure. Because of this modified procedure for the measuring transducer and the limit signal transmitter a maximum CCF detection time of 240 h and for the pressure sensing lines a maximum CCF detection time of 24 h have been assumed.

In order to take into account a simultaneous failure of several RHR legs during mid-loop operation the CCF events related to centrifugal pumps for the failure mode “no discharge“ have been newly evaluated and combined into an own set of data. The observation periods have been calculated from the annual operating times of the RHR pumps, the component cooling water pumps and the service water pumps applying the operating experience of a representative NPP with PWR and of one with BWR. For all other plants considered for the evaluation of CCF events the operating times of the

7 Level-1 PSA for low-power and shutdown operation

pumps have been calculated based on these representative times according to the reactor type and the operating time of the respective plant.

Because the operating times of the component cooling water and service water pumps and of the RHR pumps have been greatly different the reference times have been calculated applying a differentiated approach. For the component cooling water and the service water pumps as observation period the total operating time of all three groups of pumps has been chosen. For the RHR pumps as observation period the operating time of the RHR chain has been chosen, i.e. the operating period during which all three component groups were operating simultaneously. As CCF detection time the duration of the actuation of the RHR chain during this event sequence has been chosen. The CCF probabilities have been calculated for these cases applying the new "coupling model" of GRS /KRE 98/.

- **Operator actions**

As in the PSA for power operation operator actions have been evaluated by means of the THERP-approach after Swain and Guttman /SWA 83/ as recommended in the PSA Guidelines /FAK 97/.

Table 7.6 Mean values of unavailabilities of system functions and the probabilities of residual heat removal per outage

Initiating event ¹		Unavailability of		
No	Description Identification	p/out.	Un- avail.	Main contributions System functions
L.of pr. power – ext.				Restart of RHR
1	T1.1, 1B2	4.8E-4	9.8E-5	and the RHR via the SGs
2	T1.1, 1C	4.8E-4	7.1E-4	and start of the emergency core cooling chain
Failure of RHR be- cause of				
Faulty water level lowering				
3	T7.1, 1C	4.9E-6	9.4E-5	Restart of RHR and the RHR via the SGs
Failure to run of the RHR chains				
4	T7.2, 1B2	4.8E-5	2.3E-3	Start of RHR chain and the RHR via the SGs
5	T7.2, 1C	4.8E-5	1.7E-2	the RHR chain
Faulty actuation of the ECC signals				
6	T8, 1B2	7.6E-3	1.3E-4	Restart of the RHR and of the RHR via the SGs
Leak at the RHR sys- tem < 25 cm²				
in containment				
7	S8.1, 1B2	1.3E-4	2.2E-4	Restart of the RHR and of the RHR via the SGs
8	S8.1, 1C	1.3E-4	1.4E-3	and switching to IT
in annulus				
9	S8.2, 1B2	1.3E-4	2.2E-4	Restart of the RHR and of the RHR via the SGs
10	S8.2, 1C	1.3E-4	1.4E-3	and switching to IT

1) see Table 7.3

b1 Failure of RHR

b3 Failure of injection

b4 excessively high pressure in prim. circuit

d Deboration after failure of RHR

SG Steam generator

IT Injection train

CCF Common cause failure

HF Human failure

7 Level-1 PSA for low-power and shutdown operation

system damage states affecting fuel element cooling and of deborations after failure of

System functions			Probability of system damage states				Debor. d
%	Importance [%]		Fuel element cooling Failure cause			Total	
	CCF	HF	b1	b3	b4		
100	41	28	4.7E-8			4.7E-8	2.2E-9
100	38	28	3.4E-7			3.4E-7	
100	80	99	< E-9	< E-9		< E-9	< E-9
100	97	13	1.1E-7	< E-9		1.1E-7	3.3E-8
100	97	10	8.1E-7			8.1E-7	
79	2	100	1.0E-6		< E-9	1.0E-6	
100	5	83	2.7E-8	< E-9		2.7E-8	< E-9
100	3	84	1.8E-7	< E-9		1.8E-7	
100	5	68	2.7E-8	< E-9		2.7E-8	< E-9
100	3	68	1.8E-7	< E-9		1.8E-7	
Total	40	60	2.7E-6	< E-9	< E-9	2.7E-6	3.5E-8

Unavail. Total unavailabilities
 RHR Residual heat removal
 p/out. Probability per outage

Triggering events
Initiating events
System damage states
Core damage states
Release categories

Skill based and rule based actions can be analyzed and evaluated by means of the THERP method. Knowledge based actions can be evaluated only if the probability is to be quantified, that diagnostic tasks are not successfully performed within a given time interval. For the analyses of initiating events in low-power and shutdown operation frequently operator actions have to be evaluated, which are pre-planned in less detail than for power operation. This means explicitly first of all, that no written instructions are available, on which criteria actions have to be initiated, how they have to be performed and when they have to be finished.

To evaluate the reliability of such actions it has first been investigated, how far the procedure supported by operational practice or by operator training can be attributed to the rule based category (sub-category "internalized rules"). It has been taken into account, if actions which are well-known to the operators from power operation have to be performed under varying circumstances during low-power and shutdown operation.

To define operator actions low-power and shutdown operation in an improved formal manner in the existing instructions, the operator has extended the plant documentation. The extended plant documentation has been considered in investigations.

7.4.2 Loss of preferred power - external (mid-loop-operation, RPV closed)

- **Required system functions**

In mid-loop operation the residual heat is removed by two RHR system legs, operated via the RHR control valves with reduced flow rate. After shutdown the plant remains for about 20 h in mid-loop operation with a pressure-tight closed reactor pressure vessel. The operating manual defines the permissible variants for the minimal available system functions during reduced water level and „pressure-tight closed reactor pressure vessel". Required are at least three RHR system legs and on ECCS leg. One of the RHR system leg has to be in stand-by for refilling. Additionally six accumulators in stand-by for injection and one steam generator for residual heat removal are available.

To cope with the initiating event the emergency power diesels of the emergency power grid are automatically started and subsequently the RHR chains are reconnected. The failure of reconnection has been investigated by thermohydraulic analyses, to evaluate the success criteria. In this case the RHR chain in stand-by for refilling can be switched to residual heat removal operation or the ECCS chain can be activated. For this pur-

pose the mass flow rate has to be increased to the required amount. If also these means of RHE fail, the residual heat can be removed via the steam generator in stand-by. Steam generator feeding is provided by the related emergency feedwater leg, the steam is relieved via the steam relief control valve in operational mode. The thermohydraulic analyses show, that in this case – in order to avoid deboration of the coolant – the primary circuit has to be filled to a pressurizer level $L_P > 3$ m from a borated water storage tank or from at least two accumulators. If the steam relief via the steam relief control valves fails, the steam can also be relieved under high pressure via the steam relief safety valve. Should the power supply by the emergency power grid 1 fail, the emergency power diesels of the emergency power grid 2 will be started. In this case only the ECCS chain can be used for the RHR.

- **Probabilities of system damage states**

For the transition from the initiating event “loss of preferred power – external” in the plant operational state 1B2 to system damage states for the system damage state affecting the fuel element cooling a probability of $9.8 \cdot 10^{-5}$ and for the system damage state of deboration a probability of $4.6 \cdot 10^{-6}$ has been evaluated. With a probability of $4.8 \cdot 10^{-4}$ for the initiating event in plant operational state 1B2 this results in a probability of $4.7 \cdot 10^{-8}$ for system damage states of fuel element cooling and a probability of $2.2 \cdot 10^{-9}$ for system damage states of deboration.

- **Characteristics of system damage states**

The system damage states of fuel element cooling are dominated by the failure to re-establish the RHR systems and the residual heat removal via the steam generator. A damage state under medium pressure in the primary circuit will result after > 3 h if the steam generator is dry, and after > 6 h if the steam generator is flooded.

A system damage state of deboration occurs under the condition of residual heat removal via the steam generator if the primary circuit is not filled up. After about 2 h nearly completely deborated coolant will condensate in the steam generator and after about 4 h about 5 Mg of deborated coolant will have accumulated in the pump suction line and about 15 Mg in the steam generator. Thermohydraulic analyses to investigate the mixing behavior of the deborated coolant during the transport into the core and

analyses of the reactivity response of the core have been initiated. However, the possible extent of a core damage can not be evaluated up to now.

- **Contributions of system function failures**

The essential contributions to the transition probabilities come from the system functions providing the residual heat removal. A failure of fuel element cooling can occur only if these system functions fail. The contribution of the system functions

- restart of the RHR systems,
- switching of the stand-by leg to RHR function,
- start of an ECCS chain and
- RHR via one steam generator

to the failure combinations therefore is 100 % in all cases. This means, that these system functions are found in all minimal cuts, leading to a system damage state.

The same is true for the transition probability to a system damage state of deboration, because also here first the residual heat removal via the RHR chains has to fail. Additionally those system functions contribute with an importance of 100 % each, which are used to refill the primary circuit (fill-up with the stand-by leg and fill-up with the accumulators). This means, the system functions are found in all minimal cuts which lead to a system damage state of deboration.

- **Contributions of individual failure causes (importances)**

CCFs contribute 41 % and human errors 28 % to the failure causes. After this initiating event the required system functions are actuated automatically (start of the emergency power diesels and re-start of the RHR chains). Therefore operator errors do not dominate the result and CCFs are more relevant than operator errors. A failure of all four D1-emergency power diesels contributes as CCF with an importance of 13 % to the unavailability. Operator actions become important only if the automatic actions fail.

The individual contributions to the failure of the residual heat removal with the RHR chains do not show any strongly dominating influences. The highest contributions come from the operational failure of a emergency service water system pump (importance 38 %) and the start-up of the ECCS (importance 27 %).

Contributions leading to a failure of the RHR system have an importance of 10 to 18 %. This comprises, e.g., a failure of the start signal of the RHR system, a failure to open of the check valve in the suction line of the RHR system and a failure to start of the component cooling water system.

The failure of heat removal with the steam generator is caused with an importance of 42 % by an operational failure of the emergency feedwater pump and with an importance of 20 % by an operational failure of the emergency diesel in pump operation.

Operator errors during fill-up of the primary circuit contribute 95 % to the system damage state of deboration.

7.4.3 Loss of preferred power (mid-loop operation, RPV open)

- **Required system functions**

Also with an open reactor pressure vessel mid-loop operation is sustained for about 20 h using two RHR legs at reduced flow rate. Except the steam generator, which is not available for the residual heat removal in this plant operational state, the same system functions are available as in plant operational state 1B2 (section 7.4.2).

The measures required to cope with the event are essentially the same as for the operation state 1B2, with the exception that the residual heat removal via the secondary system is no longer possible. This means that with an open reactor pressure vessel a deboration of the primary coolant by condensation within the steam generator cannot occur. As with the closed reactor pressure vessel one of the possibilities to remove the residual heat with the RHR chains has to be activated in order to cope with the event. If the RHR fails, the primary coolant inventory will evaporate into the containment. Flooding of the primary circuit from the borated water storage tank resp. the accumulators will extend the period of time, available for counter measures, e.g. repair of failed components.

- **Probabilities of system damage states**

For the transition from the initiating event "loss of preferred power – external" in plant operational state 1C to a system damage state of fuel element cooling a probability of

$7.1 \cdot 10^{-4}$ has been evaluated. With a probability of $4.8 \cdot 10^{-4}$ for the initiating event to occur in plant operational state 1C this results in a probability of $3.4 \cdot 10^{-7}$ for system damage states of fuel element cooling. Because in this plant operational state the steam generator cannot be used for residual heat removal, the probability of system damage states is by a factor of 7.2 higher than for plant operational state 1B2.

- **Characteristics of system damage states**

The system damage states are determined by the failure to start of system functions for residual heat removal resp. coolant injection. After 3 - 4 h with a transition probability of $5.1 \cdot 10^{-4}$ a damage state with low pressure and open primary circuit will be reached caused by a failure of residual heat removal. If the coolant injection from the borated water storage tank or the accumulators fails a system damage state will be reached already after 2 - 3 h. The transition probability for this state is $2.0 \cdot 10^{-4}$.

- **Contributions of system function failures**

Also for this event the essential contributions to the transition probability come from those system functions which provide the possibility of residual heat removal. The fuel element cooling will fail only if all these system functions fail. Therefore the system functions

- restart of the residual heat removal systems,
- switching of the stand-by leg to residual heat removal function and
- start of one residual heat removal chain

participate in each case to 100 % in the failure combinations, as for the analogous initiating event in plant operational state 1B2 (section 7.4.2).

The failure to fill-up the reactor pressure vessel until the head flange contributes to the system damage states with an importance of 29 %.

- **Contributions of individual failure causes (importances)**

Common cause failures contribute 38 % and operator errors contribute 28 % to the system function failures. Also in this plant operational state the system functions are

actuated automatically, so that the contribution of operator errors to the result likewise is low.

The individual contributions to the failure of the residual heat removal with the RHR chains do not show any strongly dominating influences. The highest contributions come from the operational failure of the emergency service water pump with an importance of 38 % and the start of the ECCS with an importance of 27 %.

Contributions which lead to a failure of the RHR system have an importance of 10 – 18 % as for the analogous initiating event in plant operational state 1B2 (section 7.4.2). They comprise also for an open reactor pressure vessel the failure of the start signal of the RHR system, the failure to open of the check valve in the suction line of the RHR system and the failure to start of the component cooling water pump.

7.4.4 Loss of RHR by faulty water level lowering (water level lowering to mid-loop operation, RPV closed)

- **Required system functions**

As initiating events failures of the mid-loop level measurement or a failure to close the LP-reducing station during lowering the level to mid-loop are assumed (see Table 7.4). As a result of a too low level both operating RHR system legs take in nitrogen from the primary system and fail.

To cope with this event the primary circuit has to be filled up by the RHR system leg in stand-by for injection to a pressurizer water level $L_P > 3$ m and the injection leg has to switch to residual heat removal with a sufficiently high coolant flow rate. Alternatively the water level can be raised by injection from 2 out of 3 accumulators. If the injection leg can not be switched into residual heat removal function, either the ECCS leg in stand-by has to be activated or the legs which have been operated previously have to be vented and re-started.

If the residual heat removal with the RHR chains fails a steam generator with the secondary side emergency feedwater supply is available for residual heat removal. The steam is relieved via the steam relief control valve in operational mode. To avoid a deboration of the primary coolant, the fill-up of the primary circuit must have been suc-

cessful. If the steam relief via the steam relief control valve fails, the steam can be relieved at high pressure via the main steam safety valve.

- **Probabilities of system damage states**

For the transition from the initiating event "loss of residual heat removal caused by faulty water level lowering" into a system damage state of fuel element cooling a probability of $9.4 \cdot 10^{-5}$ has been evaluated. With a probability of $4.9 \cdot 10^{-6}$ for the initiating event to occur during water level lowering the system damage state of fuel element cooling has a probability of $< 1 \cdot 10^{-9}$. The transition probability for system damage states of deboration is $2 \cdot 10^{-7}$. This results in a probability $< 1 \cdot 10^{-9}$ for this system damage state.

- **Characteristics of system damage states**

The system damage states of fuel element cooling are determined by a situation, in which the primary circuit cannot be filled up or the residual heat removal with the RHR chains cannot be started after the primary circuit has been filled up. The first case leads to a damage state with medium primary circuit pressure already after 1 - 2 h. In the second case the time to reach a damage state would be 3 h if the steam generator is full and 6 h if the steam generator is empty due to a fault.

- **Contributions of system function failures**

Also for this event the essential contributions to the transition probabilities come from those system functions which can be used for residual heat removal. The fuel element cooling will fail only if all these system functions fail. Therefore the system functions

- switching the stand-by leg to residual heat removal operation,
- restart of the residual heat removal systems and
- residual heat removal via the steam generator

in each case participate to 100 % in the failure combinations.

- **Contributions of individual failure causes (importances)**

Common cause failures contribute 80 % and operator errors 99 % to the system function failures. The high contribution of operator errors can be attributed to the fact that no automatic measures are available to cope with the initiating event. The contribution from common cause failures is also high, because this failure mechanism is of high relevance already for the initiating event, as, e.g., the common cause failure of the measuring transducers. The fault tree of the initiating has to be integrated into the complete fault tree because of the dependencies of the system functions. Therefore the total result shows the same relevance.

Because of the low relevance of the event compared to other initiating events, the contributions of individual failure causes are not further discussed.

7.4.5 Loss of residual heat removal by operational failure of the residual heat removal chains (mid-loop operation, RPV closed)

- **Required system functions**

As initiating events failures of both operating residual heat removal chains are assumed (see Table 7.4). The minimal requirements for the system functions laid down in the operating manual are the same as in plant operational state 1B2 (see section 7.4.2). Thermohydraulic analyses have been performed to evaluate the success criteria for these system functions, specified below.

To cope with the initiating event the primary circuit has to be filled up to a pressurizer water level $L_p > 3$ m from one borated water storage tank or from at least two out of six accumulators. To reestablish the residual heat removal the RHR chain in stand-by for injection can be switched to RHR mode or the emergency RHR chain can be activated. For this purpose the mass flow rate has to be increased to the required value. If these alternatives for RHR should fail, the residual heat can be removed via the steam generator which is in stand-by mode. The steam generator is fed by the related emergency feedwater system leg, the steam is relieved via the steam relief control valve in operational mode. In this case successful fill-up of the primary circuit prevents a deboration of the primary coolant. If the steam relief via the steam relief control valve fails, the steam can be relieved under high pressure via the main steam safety valve.

- **Probabilities of system damage states**

For the transition from the initiating event "loss of residual heat removal by a failure of the RHR chains during operation" in plant operational state 1B2 into a system damage state of fuel element cooling a probability of $2.3 \cdot 10^{-3}$ has been evaluated, for the transition into a system damage state of deboration a probability of $6.5 \cdot 10^{-4}$ was found. With a probability of $4.8 \cdot 10^{-5}$ for the initiating event to occur in plant operational state 1B2 the probability for system damage states of fuel element cooling is $1.1 \cdot 10^{-7}$ and the probability for system damage states of deboration is $3.3 \cdot 10^{-8}$.

- **Characteristics of system damage states**

The system damage states of fuel element cooling are determined by the failure of the alternatives for RHR with the RHR chains and of the residual heat removal via the steam generator. If the steam generator was empty, a damage state under medium pressure in the primary circuit will be reached after > 3 h, if the steam generator was full after > 6 h. If also the fill-up of the primary circuit fails, the damage state will be reached already after 1 - 2 h. However the transition probability for this damage state is negligible.

A system damage state of deboration occurs if the residual heat is removed via the steam generator and the primary circuit is not filled up, as described in section 7.4.2.

- **Contributions of system function failures**

The essential contributions to the transition probability come from system functions, which provide the possibility for residual heat removal. The system functions, providing residual heat removal, like

- switching of the stand-by leg into RHR function,
- start of a emergency core cooling chain or
- residual heat removal via a steam generator

contribute with an importance of 100 % to the damage state.

For the system damage states of deboration all system functions required to fill up the primary circuit contribute with an importance of 100 % to the result.

- **Contributions of individual failure causes (importances)**

Common cause failures contribute 97 % and operator errors contribute 13 % to the system function failures. The high contribution of common cause failures can be attributed to the fact that already the initiating event is determined to 91 % by CCF leading to a failure of RHR. Because of this high contribution, and since possibilities of repair have not been considered, the contribution from operator errors is low.

The CCF (4 out of 4) of the service water pumps contributes 43 %, the CCF (4 out of 4) of the RHR pumps contributes 25 %, and the CCF (3 out of 4) of the RHR pumps contributes 14 % to the failure of residual heat removal with the RHR chains.

The contributions to the failure of residual heat removal with the steam generator and to the system damage state of deboration are the same as for the event T1.1, 1B2 (see section 7.4.2).

7.4.6 Loss of residual heat removal by failure of the RHR chains during operation (mid-loop operation, RPV open)

- **Required system functions**

Initiating events with a failure of both RHR chains in operation have been investigated also for an open reactor pressure vessel (see Table 7.4). The success criteria of the system functions are the same as in plant operational state 1B2 (see section 7.4.5).

The measures required to cope with the event are essentially the same as for plant operational state 1B2, however the residual heat cannot be removed with the secondary system. Therefore to cope with the event one of the alternatives for residual heat removal with the RHR chains has to be activated. If the residual heat removal fails the coolant inventory evaporates into the containment. The time period available for countermeasures can be extended by filling up the primary circuit from the borated water storage tank or from the accumulators.

- **Probabilities of system damage states**

For the transition from the initiating event "loss of residual heat removal by a failure of the RHR chains during operation" in plant operational state 1C to a system damage state of fuel element cooling a probability of $1.7 \cdot 10^{-2}$ has been evaluated. With a probability of $4.8 \cdot 10^{-5}$ for the initiating event to occur in plant operational state 1C the probability of system damage states of fuel element cooling is $8.1 \cdot 10^{-7}$. Because in this plant operational state the residual heat cannot be removed via a steam generator, the probability of system damage states is increased by a factor of about 7.4 compared to the analogous event in plant operational state 1B2 (section 7.4.5).

- **Characteristics of system damage states**

The system damage states are determined by a failure to start system functions for residual heat removal resp. injection. The failure of the residual heat removal leads after 3 - 4 h to a damage state with low pressure and open primary circuit with a transition probability of $1.7 \cdot 10^{-2}$. A failure to inject coolant from the borated water storage tank or the accumulators leads to a damage state already after 2 - 3 h. The transition probability of this state is $5.8 \cdot 10^{-6}$.

- **Contributions of system function failures**

Also for this event the essential contributions to the transition probabilities come from system functions which provide possibilities of residual heat removal. The fuel element cooling fails only if all these system functions fail. Therefore the contribution of the system functions

- switching the stand-by leg to residual heat removal function and
- start of an emergency core cooling chain

to the failure combinations in any case is 100 %.

The failure to refill the reactor pressure vessels until the head flange contributes to the result with an importance of 1 %.

- **Contributions of individual failure causes (importances)**

As for the analogous event in plant operational state 1B2 (section 7.4.5) - and for the same reasons – common cause failures are strongly dominating (with 97 %) and the influence of operator errors is small (10 %).

The individual contributions to the failure of residual heat removal with the RHR chains are dominated also by the CCF (4 out of 4) of the service water pumps with 44 %, the CCF (4 out of 4) of the RHR pumps with 23 %, and the CCF (3 out of 4) of the RHR pumps with 15 %.

7.4.7 Loss of residual heat removal by faulty actuation of the emergency core cooling signals (mid-loop operation, RPV closed)

- **Required system functions**

The initiating event can occur during lowering the water level to mid-loop, if the corresponding reactor protection signals are enabled at this point of time. Because of a failure to disable the signal “pressurizer level < 2,28 m“ the emergency core cooling signals are activated and all residual heat removal systems are switched into “injection“ function. The minimum system function requirements fixed in the operator manual are the same as for plant operational state 1B2 (see section 7.4.2).

To cope with the initiating event the emergency core cooling signals have to be reset, the extra borating pumps have to be switched off, and the residual heat removal has to be reestablished. If the reset of the emergency core cooling signals fails, the pressure limitation of the primary circuit and the residual heat removal via the steam generator are required. For the residual heat removal via the steam generator the emergency feedwater leg and the steam relief are required (see section 7.4.2). A system damage state of deboration cannot occur from this initiating event, because the primary system is filled up already by the initiating event itself.

- **Probabilities of the system damage states**

For the transition from the initiating event „loss of residual heat removal by faulty actuation of the emergency core cooling signals“ in plant operational state 1B2 to a system

damage state of fuel element cooling a probability of $1.3 \cdot 10^{-4}$ has been evaluated. With a probability of $7 \cdot 10^{-3}$ for the initiating event to occur in plant operational state 1B2 the probability for plant operating states of fuel element cooling is $1.0 \cdot 10^{-6}$.

After completion of the investigations it has been found, that the operational pressure limitation in plant operational state 1B2 occurs at a higher pressure than assumed in the analyses. In this case at a pressure > 3.1 MPa additional measures are necessary in order to restart the RHR chains, which have not been considered in the present analysis. The influence of these modified conditions on the PSA results have not yet been investigated.

- **Characteristics of system damage states**

This initiating event can lead to different system damage states of fuel element cooling, which are determined by a failure to restart the residual heat removal with the RHR chains and to remove the residual heat via the steam generator. With a transition probability of $1.2 \cdot 10^{-4}$ after 3 resp. 6 h, with an empty resp. a full steam generator, a damage state with medium pressure in the primary circuit will be reached. A system damage state with high primary circuit pressure, caused by a failure of the operational pressure limitation, has a transition probability of $1.2 \cdot 10^{-5}$. In this case the pressure is limited by the pressurizer safety valve. The transition probability to system damage states with a failure of the pressure limitation of the primary circuit is $< 10^{-9}$ and hence negligible.

- **Contributions of system function failures**

The essential contributions to the transition probability come from the restart of the residual heat removal with an importance of 89 % and from the residual heat removal via a steam generator with 100%. The reset of the emergency core cooling criteria, the switch-off of the extra borating pumps and the pressure limitation contribute 10 % each to the transition probability.

- **Contributions of individual failure causes (importances)**

Common cause failures contribute only 2 %, operator errors contribute 100 % to the system function failures. The contribution of common cause failures is low, because

operator actions to reset the emergency core cooling signals and to restart the residual heat removal are strongly dominant. Contributions to the common cause failures come only from the failure to start the emergency feedwater diesels for the feedwater supply of the steam generator. A failure of the emergency feedwater pump during operation contributes with an importance of 42 %, a failure of the emergency feedwater diesel generator during operation contributes with an importance of 19 % to the transition probability.

7.4.8 Leak at the residual heat removal system in the containment and in the annular room < 25 cm² (mid-loop operation, RPV closed)

- **Required system functions**

As mechanisms leading to a leak during low-power and shutdown operation vibrations, cyclic thermal stress and maintenance errors have been assumed. A leak causes the primary circuit water level to drop until the RHR chains in operation take in nitrogen from the primary circuit and fail. Leaks in the containment and leaks in the annular room initially have been investigated separately because the possibilities to detect the leak are different for both cases. However, if the extended plant documentation of the plant operator is considered this influence is negligible and both leak locations can be treated together. The success criteria of the system functions are the same as described in section 7.4.2.

To cope with a leak in a leg of the RHR system a fill-up of the primary system with the injection leg until a pressurizer water level $L_P > 3$ m, the switching of the injection leg to residual heat removal, and the restart of the intact RHR system leg after detection of the leaking leg is necessary. Alternatively the fill-up can also be performed with the accumulators, and the residual heat can be removed either with the emergency core cooling leg or over the available steam generator. If the residual heat is removed via the steam generator the primary circuit has to be filled up in order to avoid a deboration of the primary coolant.

- **Probabilities of the system damage states**

For the transition from the initiating event “leak at the RHR system in the containment“ in plant operational state 1B2 to a system damage state of fuel element cooling a prob-

ability of $2.2 \cdot 10^{-4}$ has been evaluated, for the transition to a system damage state of deboration the probability is $5.4 \cdot 10^{-6}$. With a probability of $1.3 \cdot 10^{-4}$ for the initiating event in plant operational state 1B2 the probability for system damage states of fuel element cooling is $2.7 \cdot 10^{-8}$, the probability for system damage states of deboration is $< 10^{-9}$. The same transition probabilities have been evaluated for the “leak in the RHR system in the annular room”.

- **Characteristics of the system damage states**

Two different kinds of system damage states can occur, which are characterized by a failure of residual heat removal or by a failure of coolant injection. A failure of residual heat removal leads to a damage state with medium pressure in the primary circuit after 3 resp. 6 h, with an empty resp. a full steam generator, with a transition probability of $2.2 \cdot 10^{-4}$. A failure to fill up the primary circuit leads to a damage state already after 1 – 2 h with a transition probability of 2..

The probability of a system damage state of deboration is negligible.

- **Contributions of system function failures**

The essential contributions to the transition probability come from the system functions for the residual heat removal. The system functions

- switching of the stand-by leg to RHR function,
- restart of the intact RHR leg and
- residual heat removal via a steam generator

each contribute with 100 % importance.

- **Contributions of individual failure causes (importances)**

Common cause failures contribute with 5 %, operator errors contribute with 83 % to the system function failures. The high contribution of operator errors can be attributed to the fact, that the system functions required to cope with this initiating event are not activated automatically.

Independent failures significantly contribute to the result: the failure of the operator actions to restart the intact RHR leg with an importance of 66 %, the failure to open of the check valve in the suction line of the RHR system with an importance of 32 % and the failure to open of the first isolating valve with an importance of 19 %. Further independent failures follow with lower importances.

The essential contributions to the failure of the residual heat removal via the steam generator come from the failure of the emergency feedwater pump during operation and the failure of the emergency feedwater diesel in pump operation, as described in section 7.4.2.

7.4.9 Leak at the residual heat removal system in the containment and in the annular room < 25 cm² (mid-loop operation, RPV open)

- **Required system functions**

A leak at the residual heat removal system can occur while the reactor pressure vessel is open. Also for this case the leak locations “containment” and “annular room” are treated together considering the extended plant documentation of the operator. The minimal configuration of available system functions again is identical to plant operational state 1B2. However, the steam generator is not available for residual heat removal in this plant operational state.

The measures to cope with the initiating event are the same as in plant operational state 1B2, except the residual heat removal via the secondary circuit. Therefore residual heat removal with the (intact) RHR chains has to be established to cope with the event. If the residual heat removal fails the coolant inventory evaporates into the containment. The time period available for countermeasures can be extended by filling up the primary circuit from the borated water storage tank or with the accumulators.

- **Probabilities of system damage states**

For the transition from the initiating event “leak at the residual heat removal system in the containment” in plant operational state 1C to a system damage state of fuel element cooling a probability of $1.4 \cdot 10^{-3}$ has been evaluated. With a probability of $1.3 \cdot 10^{-4}$ for the initiating event to occur in plant operational state 1C the probability for system

damage states of fuel element cooling is $1.8 \cdot 10^{-7}$. The same transition probabilities have been found for a “leak at the residual heat removal system in the annular room”. Because the steam generator cannot be used for residual heat removal in this case, the probability for a system damage state is increased by a factor of about 6.7 compared to the analogous events in plant operational state 1B2 (section 7.4.8).

- **Characteristics of system damage states**

The system damage states are determined by a failure to start system functions for residual heat removal or by a failure of coolant injection. The failure of residual heat removal leads to a damage state with low pressure and open primary circuit after 3 - 4 h with a transition probability of $1.4 \cdot 10^{-3}$. A failure of coolant injection occurs with a transition probability of $5.7 \cdot 10^{-6}$. This leads to a damage state under low pressure after 1 - 2 h.

- **Contributions of system function failures**

The essential contributions to the transition probability also in plant operational state 1C come from those system functions, which provide the possibilities for residual heat removal. The system functions

- switching of the stand-by leg to residual heat removal function and the
- restart of the intact RHR leg

each contribute with 100 % importance to the result.

- **Contributions of individual failure causes (importances)**

Common cause failures contribute 3 %, operator errors contribute 84 % to the system function failures. The high contribution of operator errors also for this initiating event is to be attributed to the fact, that the system functions are not activated automatically.

As with the closed RPV independent failures contribute significantly to the result. The importances are analogous to plant operational state 1B2.

7.5 Summarized explanations concerning the system damage states

To evaluate the methods of a PSA for low-power and shutdown operation, initiating events were investigated which are typical of low-power and shutdown operation and of which the major contributions to the system damage states of a plant in low-power and shutdown operation are expected in the light of current knowledge. These are initiating events (transients and leakages) that can lead to a failure of residual-heat removal, and events which can cause the generation of unborated water in the primary system (deborations).

- **Initiating events**

Initiating events with a failure of residual-heat removal were analyzed for mid-loop operation after cooldown of the plant with the reactor pressure vessel (RPV) closed and open. During these plant operational states (1B2 and 1C), the demands on the safety functions for fuel element cooling are highest. The highest probability has a transient by "loss of residual-heat removal due to faulty emergency cooling signals". This event did occur several times in German PWR plants. It has to be noted, that this event cannot occur, if the corresponding reactor protection signals are deactivated prior to lowering the primary system water level. With the primary system depressurized, initiating events due to leakages are only assumed to occur in the affiliated systems, e. g. due to vibrations. The probability of such leaks is comparatively low.

Initiating events which may result in an influx of unborated water from outside into the primary system (in contrast to boron dilution events by accumulation of condensate in "reflux condenser mode" after the failure of active residual-heat removal) were analyzed with regard to the probability of an influx of unborated water into the primary system. Primary-side recognition criteria, such as a level increase, and related countermeasures to limit the influx of unborated water have not been assessed. Similarly, no statements can yet be made regarding the mixing behavior up to the passage through the core nor with respect to the criticality behavior of the core. Therefore, probabilities of system damage states resp. core damage states due to the influx of unborated water into the primary circuit could not be evaluated.

- **System damage states**

At $2.7 \cdot 10^{-6}$ /a - assuming one planned outage per year -, the frequency of system damage states affecting fuel element cooling during low-power and shutdown operation is within the same order of magnitude as the frequency of system damage states during power operation. The LP&SD PSA first evaluates probabilities of system damage states per outage. Multiplication with the number of outages per year (assumption here: one outage) gives a frequency (per year), which can be compared with the results of the PSA for power operation. The contributions from individual initiating events to the total frequency and the contributions from the unavailabilities of system functions are shown in figures 7.1 to 7.4 system damage states affecting the fuel element cooling and in figure 7.5 for system damage states of deboration.

The highest contributions, estimated for initiating events not analyzed in detail, come from a "loss of main heat sink without loss of main feedwater" with $1.2 \cdot 10^{-7}$ /a and a "loss of main feedwater and main heat sink" with $1.5 \cdot 10^{-7}$ /a. If these contributions are taken into account, under the proviso of a detailed analysis the total result is slightly increased to about $3 \cdot 10^{-6}$ /a.

The dominant contribution to the above quoted total result with about $1 \cdot 10^{-6}$ /a comes from the "loss of residual-heat removal due to faulty emergency cooling signals". This event can occur only if the reactor protection system is fully activated during water level lowering. If during a planned outage the corresponding reactor protection signals are deactivated in an early phase, the total result is reduced to $1.7 \cdot 10^{-6}$ /a; for a fully activated reactor protection system the total result increases to about $6.4 \cdot 10^{-6}$ /a. In the PSA the frequencies with and without deactivation of the reactor protection signals have been weighted by the number of outages, during which in the reference plant the reactor protection signals have been deactivated or not.

The early deactivation of the reactor protection signals could be an efficient method to reduce the probability of system damage states during shutdown operation. However this question cannot be finally answered right now, because potential adverse effects of an early deactivation have not been investigated in the present PSA.

For system damage states with deboration of the primary coolant due to condensate accumulation after a loss of the active decay heat removal a frequency of $3.5 \cdot 10^{-8}$ /a has been estimated. Also this value assumes one planned outage per year.

7 Level-1 PSA for low-power and shutdown operation

System damage states occur in about 45 % of the cases with the RPV closed and in about 55 % of the cases with the RPV open (see figure 7.2). The system damage states are caused in about 85 % of the cases by transients and in about 15 % of the cases by LOCAs.

Taking their probabilities as measure, system damage states characterized by a failure of injection (b3) or inadmissibly high pressure in the RPV (b4) are negligible compared to system damage states caused by a loss of residual-heat removal (b1). The minimum periods after which core heat-up can begin lie between about 1 h and approx. 6 h. If one takes credit of further residual-heat removal options, core heat-up begins after about 10 h.

Concerning the transients, the initiating event "loss of residual-heat removal due to operational failure of the RHR chains" makes the dominating contribution for the plant operational state 1C under the condition "RPV open". This can be mainly attributed to the failure of residual-heat removal as a result of a common cause failure and the lack of alternative methods of residual-heat removal (e.g. via a steam generator). In plant operational state 1B2 under the condition "RPV closed", the initiating event "loss of residual-heat removal due to faulty emergency cooling signals" represents the dominating contribution among the transients to the system damage states. Here, the system damage states are mainly characterized by a failure to restore the residual-heat removal.

Only in the case of plant operational state 1C with open RPV the LOCAs cause significant contributions to the system damage states (approx. 22 %). From plant operational state 1B2 with closed RPV the contribution to the probability of system damage states is merely about 4 %. This can be attributed to the fact that with the closed RPV residual-heat removal can still be performed via the steam generator once the leak has been isolated. The location of the leakage (in the annular room or in the containment) has no effect on the result, because the plant documentation provided by the utility does not initially require leak detection.

The frequency of system damage states due to deboration by condensate accumulation during passive residual-heat removal in "reflux condenser mode" following a failure of residual-heat removal via the RHR chains is dominated to about 95 % by the initiating event "loss of residual-heat removal due to operational failure of the RHR chains".

In this case refilling of the primary circuit with the stand-by RHR train in order to avoid deboration is also not possible.

The total result is influenced by CCF contributions with an importance of 40 %. This contribution varies between 2 and 97 % for the ten investigated initiating events (see table 7.6). Especially for the LOCAs the CCF contribution is low, because in these cases redundant systems are not required. Human errors contribute significantly to the results with the exception of loss of normal ac-power (automatic reconnection of the systems) and of operational failure of the RHR chains. The importance of human errors related to the total result is about 60 %. For a “loss of decay heat removal by operational failure” the influence of human errors is low, because the CCF of components is dominating.

The investigations of low-power and shutdown operation have shown that the system damage states during these plant operational states cannot be neglected compared with power operation and that the methods a PSA for power operation can be applied to these plant operational states if specific supplements are added.

For an interpretation of the results it has to be considered, the primary objective of the investigations was the evaluation of the methods. A comprehensive level 1 PSA for low-power and shutdown states could largely apply the same methods as the present PSA, but would require significantly higher effort. New methodical requirements could result from an investigation with about $1 \cdot 10^{-6}$ /a of internal and external area events which have not been considered in the present PSA.

7.6 Uncertainties of the reliability analysis

In the quantitative analyses with regard to low-power and shutdown operation, the epistemic uncertainties concerning the probability of the initiating resp. triggering events and the reliability data for the system components and manual actions are treated in the same way as in the level 1 PSA for power operation (see Section 5.4).

The uncertainties of failure rates resp. failure probabilities up to have generally been described by adapted lognormal distributions. During the analysis it turned out to be more meaningful to use Gamma distributions for failure rates and Beta distributions for failure probabilities. The corresponding modifications have been realized in the present PSA for one operational transient and for selected operator actions with dominant con-

7 Level-1 PSA for low-power and shutdown operation

tributions and for the probability of an initiating event. Finally the following distributions have been used:

- Gamma distribution for the frequency of occurrence of operational transients (external loss of normal ac-power),
- Lognormal distribution for
 - the probability of leaks,
 - failure rates of component functions,
 - failure probabilities of component functions,
- Beta distributions for
 - probabilities for operator errors (selected actions),
 - the probability of the initiating event “loss of decay heat removal by faulty actuation of the emergency cooling signals”.

A general conversion of all lognormal distributions has not been performed in the present PSA.

• Results of the uncertainty analysis for system damage states

The results of the uncertainty analysis for the probability of system damage states affecting the fuel element cooling are shown in table 7.7 and for the probability of deboration in Table 7.8. The tables are displaying the 5 % -, 50 % -, and 95 % - fractiles of the subjective probability distributions and the point values and mean values of the individual initiating events and of the total value of system damage states. In figure 7.6 these results (excepted the point values) are graphically displayed in a logarithmic scaling.

An indicator for the result uncertainty of the evaluated probabilities of system damage states is the factor between the 95 % - fractile and the 50 % - fractile (“spread factor”). As can be seen from figure 7.6 these uncertainties are strongly varying for the individual initiating events. The spread factor is about 5 – 9 for transients (T1.1 – t(9), about 15 – 18 for LOCAs and about 12 and 180 for system damage states of deboration. For the deboration the subjective probability distributions are strongly asymmetrical. The factors between the 95 % - and 5 % - fractiles are here 275 and 930.

The higher spread factors for LOCAs are caused by the relatively large uncertainties of the probability of occurrence of these initiating events. The spread factor here is already about 10. This indicates that failure combinations of several components with coupled reliability data do not significantly contribute to the result. Nevertheless also for the LP&SD PSA point values should not be used as representative results.

For system damage states of a deboration the large spread factors are attributed to two operator actions with coupled failure rates. The uncertainty about these actions is Beta-distributed, and the actions – especially for the event T7.2, 1B2 – contribute strongly to the result.

The results of the uncertainty analysis for the total frequency of system damage states (SDS-FE and SDS-D) can be seen from the bottom lines of the tables 7.7 and 7.8 and from the last column in figure 7.6. For the system damage state affecting the fuel element cooling the difference between point value and mean value is small and the factor between 95 % - and 5 % - fractile is about 16. For the system damage state of deboration point value and mean value behave like for the event T7.2, 1B2, which essentially dominates the total result. The factor is here about 1.35. The factor between 95 % - and 5 % - fractile is 625 and is also determined by the event T7.2, 1B2.

7.7 Findings related to PSA methods and systems engineering

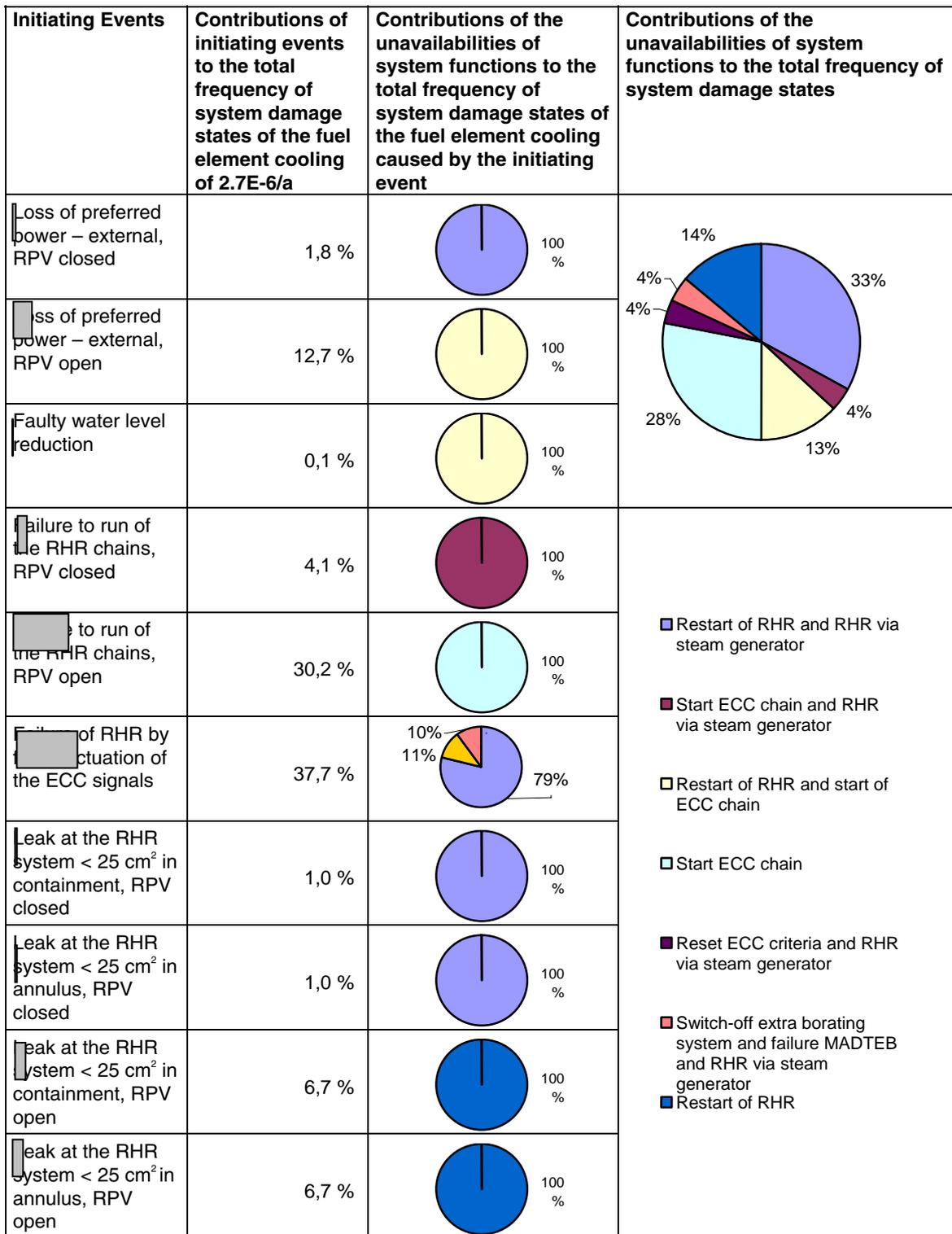
7.7.1 PSA methods

With regard to the methods of a Level-1 PSA for low-power and shutdown operation, the work for the present PSA has yielded new insights:

- Generally, it is possible to use the available methods of a PSA for low-power and shutdown operation if specific adaptations are made. The adaptations concern:
 - the analysis of the outage sequence for the identification of plant operational states,
 - the determination of outage-specific triggering and initiating events and their probabilities of occurrence,
 - the adaptation of common cause failure data to the specific operational conditions,

7 Level-1 PSA for low-power and shutdown operation

- the analysis and evaluation of operator actions as far as performed on the basis of operational practice, and
- the evaluation of the time-dependent unavailabilities of technical system during a planned outage.



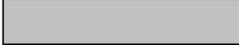
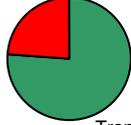
MADTEP Coolant mass-, -pressure- and temperature-gradient-limitation

RHR Residual heat removal
RPV reactor pressure vessel

Fig. 7.1 Initiating Events
Contributions of initiating events to the total frequencies of system damage states of the fuel element cooling
Contributions of unavailabilities of system functions

7 Level-1 PSA for low-power and shutdown operation

- The investigations are based on a typical two-week refueling outage of the reference plant and concentrate on initiating events that are typical of low-power and shutdown operation. In order to complete the investigations and to back up the results it is therefore necessary to review the plant operational states and the work performed for other plant outages as well. Such an outage may e. g. be a week-long short outage to move fuel elements without unloading the core or a four-week outage with an RPV pressure test. In this context it will have to be checked whether during these outages any triggering or initiating events can occur which are not covered by the existing spectrum. Furthermore the validity of the assumption has to be examined, that the analyzed initiating events from the existing spectrum deliver the essential contributions to the system damage states. For this purpose, further thermal-hydraulic analyses concerning plant behavior after initiating events during shutdown or start-up as well as estimations of the contributions to the system damage states are required.

State of the primary circuit	Contributions of initiating events to the total frequency of system damage states of the fuel element cooling of 2.7E-6/a with closed / open RPV	Contributions to the total frequency of system damage states of the fuel element cooling from transients and LOCAs with closed / open RPV
RPV closed	 45 %	LOCAs 4 %  Transients 96 %
RPV open	 55 %	LOCAs 24 %  Transients 76 %

RPV reactor pressure vessel

Fig. 7.2 Initiating Events
 Contributions of initiating events to the total frequency of system damage states of fuel element cooling with closed/open RPV
 Contributions of system damage states from transients and LOCAs

Initiating event	Contributions of the initiating events to the total frequency of system damage state of the fuel element cooling of 2.7E-6/a with closed RPV
Loss of preferred power – external	3,8 %
Faulty water level reduction	0,2 %
Failure to run of the RHR chains	9,0 %
Injection of water by faulty actuation of the ECC signals	82,6 %
Leak at the RHR system < 25 cm ² in the containment	2,2 %
Leak at the RHR system < 25 cm ² in the annulus	2,2 %

Fig. 7.3 Initiating events
Contributions of initiating events to the total frequencies of system damage states with closed reactor pressure vessel

- Apart from the completion of the event spectrum, another task is the analysis of the event sequences leading up to core damage states. Further steps are also necessary with regard to the analysis of initiating events with an influx of unboiled water into the primary system. These events require a probabilistic assessment of those measures which can limit an injection by way of measures taken in response to indications from the primary system. To assess these events with regard to their potential for fuel element damage, the thermal-hydraulic and neutron-kinetic models first need to be developed further.

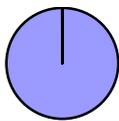
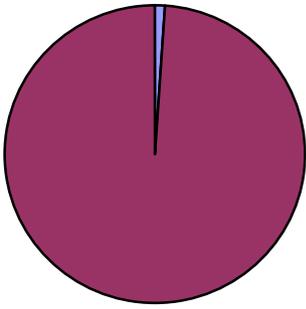
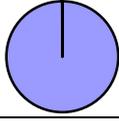
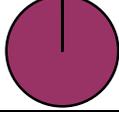
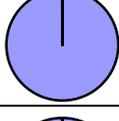
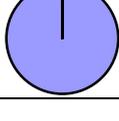
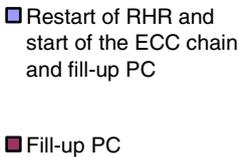
	Initiating event	Contributions of the initiating events to the total frequency of system damage state of the fuel element cooling of 2.7E-6/a with open RPV
	Loss of preferred power – external	22,5 %
	Failure to run of the RHR chains	53,6 %
	Leak at the RHR system < 25 cm ² in the containment	12,0 %
	Leak at the RHR system < 25 cm ² in the annulus	12,0 %

Fig. 7.4 Initiating events
Contributions of initiating events to the total frequency of system damage states with open reactor pressure vessel

- A need for further methodical development is also seen for the assessment of operator actions. This applies in particular to the methodical procedure and the database relating to actions with little pre-planning (actions with dominating cognitive proportions). Such actions will always play a role in the control of initiating events, even if the most important procedures are laid down in the operating manual. In connection with method development it is essential that also the damage-increasing potential of these actions be considered and that apart from the assessment methodology, the database be developed as well. A further potential for development is seen in the assessment of personnel actions in the case of long time periods and the associated correction options as well as with regard to the modeling of influencing organizational factors. The creation of a database for the assessment of such influencing factors should be closely linked to operating experience. In analogy to the component database, it would be desirable for the purpose of a realistic assessment to back up the entire personnel actions database with the help of current operating experience. GRS is presently pursuing first steps in this direction.

- Independent of the work yet to be done to complete and back up the methodology, the investigations of low-power and shutdown operation should be inte-

grated into the periodic safety reviews. This is advisable simply due to the contribution of the initiating events to the system damage states which, compared to the system damage states from power operation, cannot be neglected. A further important argument, however, is the systematic method with which the procedure to control the initiating events under the different boundary conditions of the event sequences is analyzed.

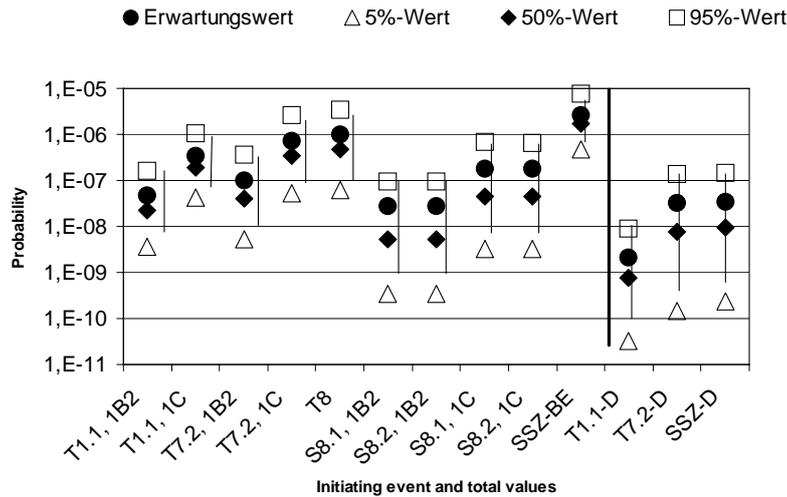
Initiating Event (RPV closed)	Contributions of the initiating events to the total frequency of system damage state of deboration of 3.5E-8/a	Contributions of the unavailabilities of system functions to the total frequency of the system damage states of deboration caused by the initiating event	Contributions of the unavailabilities of system functions to the total frequency of system damage states of deboration
Loss of deferred power – external	6,3 %	 100 %	 1% 99%
Faulty water level reduction	0,1 %	 100 %	
chains	94,3 %	 100 %	
Leak at the RHR system < 25 cm ² in the	0,1 %	 100 %	
Leak at the RHR system < 25 cm ² in the annulus	0,1 %	 100 %	
			

RHR Residual heat removal
PC Primary circuit

RPV reactor pressure vessel

Fig. 7.5 Initiating events
Contributions of initiating events to the total frequencies of system damage states of deboration
Contributions of the unavailabilities of system functions

7 Level-1 PSA for low-power and shutdown operation



System damage states of fuel element cooling:

- T1.1, 1B2 Loss of preferred power - external, reactor pressure vessel (RPV) closed
- T1.1, 1C Loss of preferred power - external, RPV open
- T7.2, 1B2 Failure of the RHR chains to operate, RPV closed
- T7.2, 1C Failure of the RHR chains to operate, RPV open
- T8 Failure of RHR by faulty activation of the ECCS signals
- S8.1, 1B2 Leak < 25 cm² at the RHR system in the containment RPV closed
- S8.2, 1B2 Leak < 25 cm² at the RHR system in the annular room, RPV closed
- S8.1, 1C Leak < 25 cm² at the RHR system in the containment, RPV open
- S8.2, 1C Leak < 25 cm² at the RHR system in the annular room, RPV open
- SSZ-BE Total value system damage states of fuel element cooling

System damage states of deboration:

- T1.1-D System damage states of deboration from the initiating event T1.1, 1B2
- T7.2-D System damage states of deboration from the initiating event T7.2, 1B2
- SSZ-D Total value system damage states deboration

Fig. 7.6 Uncertainties of the system damage state frequencies and of their total values

Table 7.7 Fractiles, point values and mean values of the probabilities per outage of system damage states of fuel element cooling

No	Description	5 % - fractile	Median (50 % - fractile)	Point value	Mean value	95 % - fractile
1	Loss of preferred power – external (T1.1, 1B2)	3.6E-9	2.2E-8	4.4E-8	4.7E-8	1.6E-7
2	Loss of preferred power – external (T1.1, 1C)	4.3E-8	2.0E-7	3.4E-7	3.4E-7	1.0E-6
3	Faulty water level lowering (T7.1)	n.e.	n.e.	n.e.	< E-9	n.e.
4	Failure of the RHR chains to operate (T7.2, 1B2)	5.2E-9	4.1E-8	1.1E-7	1.1E-7	3.6E-7
5	Failure of the RHR chains to operate (T7.2, 1C)	5.2E-8	3.4E-7	8.1E-7	8.1E-7	2.6E-6
6	Loss of RHR by faulty actuation of ECCS signals (T8)	6.2E-8	4.8E-7	1.0E-6	1.0E-6	3.4E-6
7	Leak < 25 cm ² at RHR system in containment (S8.1, 1B2)	3.4E-10	5.4E-9	2.3E-8	2.7E-8	9.6E-8
8	Leak < 25 cm ² at RHR system in annular room (S8.2, 1B2)	3.4E-10	5.4E-9	2.3E-8	2.7E-8	9.6E-8
9	Leak < 25 cm ² at RHR system in containment (S8.1, 1C)	3.3E-9	4.5E-8	1.6E-7	1.8E-7	6.7E-7
10	Leak < 25 cm ² at RHR system in annular room (S8.2, 1C)	3.3E-9	4.5E-8	1.6E-7	1.8E-7	6.7E-7
	Total values	4.8E-7	1.7E-6	2.7E-6	2.7E-6	7.5E-6

n.e. not evaluated

Table 7.8 Fractiles, point values and mean values of the probabilities per outage of system damage states of deboration

No	Description	5 % - fractile	Median (50% - fractile)	Point value	Mean value	95 % - fractile
1	Loss of preferred power – external (T1.1, 1B2)	3.2E-11	7.6E-10	2.0E-9	2.2E-9	8.8E-9
4	Failure to operate of RHR chains (T7.2, 1B2)	1.5E-10	7.8E-10	2.4E-8	3.3E-8	1.4E-7
Total values				2.6E-8	3.5E-8	

7.7.2 Systems engineering

The PSA for low-power and shutdown operation has led to significant findings with regard to systems engineering which can also have generic relevance for other plants.

- The investigations have shown that the frequencies of system damage states during low-power and shutdown operation for plants with a very high level of safety and correspondingly low frequencies of system damage states during power operation cannot be neglected.
- The inspection intervals for important components had been chosen awkwardly, which resulted in a high unavailability.
- The measures provided to cope with initiating events could be improved - especially with the RPV closed - by making the systems more reliable, by e. g. the provision of a further RHR train on stand-by for injection.
- The specification in writing of the procedures to cope with initiating events can prevent damage-increasing actions carried out because of misinterpretations of the prevailing specific boundary conditions.
- The high contribution of the initiating event "loss of residual-heat removal due to faulty reactor protection signals" shows up the considerable relevance of the regulations concerning work carried out on the reactor protection system during sensitive plant operational states.

7.7 Findings related to PSA methods and systems engineering

- The investigations carried out so far with respect to external deboration events show the importance of a detailed concept for the prevention of an undesired insertion of unborated water into the primary system.
- The thermal-hydraulic analyses have shown the need of raising the coolant level to above mid-loop operation in order to prevent deboration due to "reflux condenser mode" mode after a failure of residual-heat removal.

8 Summarized evaluation and conclusions

It was the objective of the study, to evaluate the available methods of a probabilistic safety assessment and to demonstrate their qualification for a practical application. Chapter 8.1 discusses the insights into the available PSA methods and draws conclusions concerning their applicability and necessary developments. In chapter 8.2 insights into the safety of the reference plant – gained as "by-product" of the evaluation of PSA methods – are summarized.

8.1 Insights related to the available PSA methods

8.1.1 Results of the evaluation of PSA methods

- **Scope of the PSA**

The evaluation did comprise such methods, which can be applied without major difficulties by practitioners with adequate experiences. As far as several methods are available, the most advanced approach has been used. We did refrain from the evaluation of alternative methods. The methods evaluated in the present PSA pertain to

- the levels 1 and 2 of a PSA for normal power operation without consideration of the following influences:
 - area events caused by earthquake, extreme flooding, and extreme weather conditions
 - large failures of vessels with high energy content
 - possible core criticality caused by larger amounts of deborated coolant, produced inside, or inserted into, the primary circuit,
- the level 1 of a PSA for low power and shutdown states with the same restrictions as for the level 1 PSA for normal power operation and, furthermore, without consideration of recovery actions and plant internal accident management.

For the influences which have not been considered and for the level 2 of a PSA for low power and shutdown states methods to produce reliable results with reasonable effort, or reliable data, are currently not available.

Furthermore, in the level 2 part of the PSA – according to the objectives of the PSA – the amount of radionuclide releases has not been investigated in detail, although the methods for this analysis are available. Within these restrictions – defined mainly by the available methods – the present PSA is comprehensive.

- **Relation to the German PSA Guideline**

The methods which have been selected for evaluation generally are in accordance with the German PSA Guideline. However the extent of modifications of the Basis-PSA, which is in compliance with the PSA Guideline, makes evident, that the PSA Guideline is interpretable to a considerable degree and therefore of limited value for a plain conversion of the described methods into a PSA complying with the state of the art.

- **Evaluation of common cause failures**

A main reason for the necessary modifications was the method for the evaluation of common cause failures (CCF) applied in the basis-PSA. We are of the opinion that the CCF-model applied in the Basis-PSA – in compliance with the PSA Guideline – does not allow to reflect in a reliable manner the operational experience. With the “coupling model”, developed by GRS and used in the present PSA, a differentiated consideration of CCF relevant operational experience is possible. However, expert judgment has to be included for the quantitative turn-over of operational experience into failure rates.

In the Basis-PSA in most cases significantly lower CCF probabilities than in the present PSA have been used. Because the PSA results are very strongly influenced by the CCF probabilities, the Basis-PSA calculated very low frequencies of system and core damage states even without consideration of technical installations and measures, which have a significant safety importance from a deterministic point of view (e.g. high pressure injection in sump recirculation mode).

Furthermore the Basis-PSA used generic reliability data for single failures of components, which generally are more optimistic than the plant specific data used by GRS.

- **Accident procedures**

The Basis-PSA did not consider accident procedures which are planned in the protection goal oriented part of the operators manual (e.g. high pressure injection into the primary circuit in sump recirculation mode). Also without consideration of such procedures the Basis-PSA calculated damage state frequencies, which are lower than the orientation values given in the PSA Guideline and which, therefore, have been deemed to be sufficiently low.

The result is, that exactly that part of the operators manual was not evaluated probabilistically, which in past years played a central role in the improvement of the operator manuals in German nuclear power plants.

In the present PSA also the methods to take into account the protection goal oriented part of the operator manual have been evaluated. Thus it was also possible, to identify weak points in this part of the operator manual and in the transition from the event oriented part of the operator manual.

- **Preventive measures of the plant internal accident management and recovery**

In the Basis-PSA the plant internal accident management measure “Primary side bleed and feed” was not considered. Also the repair of safety equipment was not considered, although in the maintenance rules the repair of failed components after accident initiation is planned, if sufficient time is available. Also in these cases additional effort for the analysis has been avoided, because a further reduction of the calculated frequencies of damage states was not deemed to be necessary.

The present PSA took into account all plant internal accident management measures planned in the emergency manual. In this way it was also possible, to identify weak points in the emergency manual. Furthermore, repair of components of the start-up and

shut-down system has been included exemplary into the probabilistic evaluation, in order to evaluate the corresponding methods.

The present PSA has shown, that all measures included in the deterministic safety design should be considered in the PSA in order to identify potential deficiencies.

- **Transition from level 1 to level 2 of the PSA**

For the level 2 of the PSA, which starts from the results of level 1, the core damage states have to be characterized by all features, which can influence the further course of a core damage accident. Typical features are: duration from the initiating event to a core damage state; availability of primary side injection systems; primary system pressure at a core damage state; failure combination of systems prior to core damage. Altogether 69 core damage states with different combination of features, relevant for the accident consequences, have been identified. The method evaluated in the present PSA allows a consistent coupling of the core damage states identified in level 1 by means of event tree and fault tree analysis with event tree analysis of accident sequences in level 2. The interface has been designed in such a way, that relevant results, e.g. the frequency of large releases of radionuclides, can be traced back to failures of operational and safety systems and measures.

- **Low-power and shutdown operation**

The evaluation of methods for a low-power and shutdown PSA was restricted to level 1, not considering, however, the repair of failed safety relevant equipment and measures of preventive plant internal accident management. Keeping in mind these restrictions, the present investigations have shown, that the available methods are capable to identify weak points with concern to the control of relevant events during low-power and shutdown states. The methods have been tested by the investigation and evaluation of event sequences which can lead to a failure of the core cooling or to the formation of deborated coolant plugs in the primary circuit. These investigations have been performed only for plant operational states with relatively high system function demands. These are the plant operational states with mid-loop operation immediately after shutdown. In this way it is possible to identify safety relevant weak points, prevail-

ing during a plant outage. This requires a specific part of the operators manual, describing mainly measures to cope with failures of the decay heat removal first of all during a subcritical cold plant state. Altogether considerable effort for the adaptation and evaluation of methods is still necessary, in order to perform a PSA up to level 2 for low power and shutdown states which is equivalent to a PSA for normal power operation.

- **Result uncertainties**

For the evaluation of result uncertainties in important points methods have been applied, which are different from former PSAs and also from the requirements of the German PSA Guideline.

Up to now it was common practice, to calculate the PSA results at first as “point values” applying the mean values of the reliability data as “point values” for the input parameters. Afterwards subjective probability distributions of the results have been calculated from the subjective probability distributions of the input parameters. For this approach the effort is significantly lower than for an analysis that takes account of input parameter uncertainties in a comprehensive manner.

Although the point values are calculated from the mean values of the input parameters, they are more or less different from the mean values of the probability distributions of the results. These differences are caused by the “failure rate coupling”. If reliability parameters for several components are taken from the same data base, they are varied for the uncertainty analysis not independently, but they are “coupled”. For the point value calculation failure rate coupling cannot be taken into account.

In the present PSA unexpectedly high differences between point values and mean values of system and core damage state frequencies have been found in a number of cases. This led to the conclusion that point values should be used – if at all – only for a first rough information on the PSA results. On principle the PSA results should be calculated and displayed together with their uncertainties. This approach requires a considerably higher effort for the analysis (especially for the calculation of importances), but it delivers also information on the quality of results.

During the transition from the point value calculation to the comprehensive calculation of uncertainties it became evident, that the application of lognormal distribution (LND) applied up to now for the description of uncertainties of failure rates and failure probabilities is questionable. So for failure probabilities the problem can arise, that the LND can also deliver (senseless) values > 1 . Since also for other reasons epistemic uncertainties of failure probabilities are better described by Beta-Distributions, and of failure rates by Gamma-distributions, in future PSA Beta- resp. Gamma-distributions should be used instead of LND. In order to limit the additional effort in the present PSA only the distributions of failure probabilities (for important components) have been changed from the formerly used LND into Beta-distributions.

An indicator for the uncertainty of the PSA results is the factor between the 50 %- and the 95 %-fractile of the subjective probability distribution of the result under consideration (in the following called “spreading factor”). This spreading factor varies for the frequencies of system damage states calculated in the level 1 PSA for power operation – depending on the initiating event – between 5.7 (loss of normal ac-power) and 16.8 (small leak in the main coolant pipe, 80 – 200 cm²). Caused by averaging effects for the total value with 4.4 a smaller spreading factor is calculated than for the individual contributions. The spreading factors are about the same for the frequency of core damage states from LOCAs. For transients significantly higher spreading factors have been calculated (up to 50 for the loss of main feedwater and main heat sink). For the total core damage frequency the spreading factor is 4.9.

In the level 2 part of the PSA smaller uncertainties have been found, although very complex phenomena have to be analyzed, which often can be simulated only with greatly simplified computer codes or have to be evaluated by means of expert judgment. This result which is surprising in the first moment can be well explained by the following reasons:

- The level 1 part of the PSA is dealing with very low frequencies of occurrence (for individual sequences $< 10^{-6}$ per year). The level 2 part does investigate very unlikely events, but the low frequency of occurrence is irrelevant for the uncertainty of the results. What is important is the fact, that the evaluated conditional probabilities cover an area of about $1 - 10^{-2}$.
- Part of the input parameters of level 1 (failure rates, failure probabilities) are connected with large uncertainties. These uncertainties do not depend on the extent of operational experience, but only on the number of component failures which did ac-

tually occur. For highly reliable components the failure rate (resp. failure probability) will be very low. If no or only a few failures have been observed, large uncertainty will be found even after long term operational experience. This effect can be aggravated by the failure rate coupling.

- Most of the uncertain input parameters of the level 2 part of the PSA are based on expert. Provided that the smallest estimated value is different from 0, the factor between the largest and the smallest value (in most cases uniformly distributed) is > 10 only for a few input parameters and it is in no case > 50.
- Different from the level 1 part of the PSA there is no statistical coupling between uncertain input parameters of the level 2 part, i.e. the values are varied independently of each other for the uncertainty analysis. Averaging effects tend to further reduce the uncertainty of results.

The quantified uncertainties, which are resulting for the level 1 part from the uncertainties of initiating event frequencies and of the reliability data for components and operator actions and for the level 2 part mainly from the uncertainties of input parameters for the accident simulation, altogether are in a region, which is not uncommon for the investigation of very unlikely events. However it has to be mentioned, that the PSA results are connected with additional uncertainties which cannot, or can only partially, be quantified at the current state of the art (e.g. modeling uncertainties) or which principally cannot be quantified (e.g. negligence of unknown phenomena).

8.1.2 Conclusions concerning the evaluation of methods

Conclusions from the evaluation of methods are related on the one side to the application of the methods in practice and on the other side to the necessary development of methods, as far as important for the identification of weak points of the safety design.

8.1.2.1 Application of the available probabilistic methods

The investigations have shown, that the available methods – in spite of existing limitations – are capable to identify unknown safety relevant weak points. It is important in this context, that the methods have been evaluated for a reference plant, which is in full compliance with the current nuclear rules and regulations in Germany. Weak points have been identified mainly in those respects which are not sufficiently considered in

the rules (e.g. diversity, transition from the event oriented to the protection goal oriented part of the operator manual). This means, that a purely deterministic evaluation following the nuclear rules and regulations is not sufficient today for an evaluation of the safety status of a plant according to the state of the art. The systematic approach of the PSA points out strength and weak points of safety design and quantifies the uncertainty of the evaluation. This is not possible if only deterministic methods are used.

The investigations also show, that the application of probabilistic methods requires unambiguous guidelines. The existing German PSA Guideline is not unambiguous in important points (CCF model, data base, fire PSA), so that an equally good quality of PSAs from various performing teams cannot be guaranteed.

GRS has developed for its own purposes requirements for a level 1 PSA for power operation based on the actual state of the art. These requirements currently are being extended to a level 1 PSA for low power and shutdown states and for the level 2. Considering the importance of the PSA for the Periodical Safety Review of the German nuclear power plants universally valid requirements should be established as soon as possible, in order to guarantee the same high quality of all PSAs.

In future PSAs for the Periodical Safety Reviews at least selected events in low power and shutdown states should be investigated. This is not only international practice, but it is also necessary to identify and eliminate weak points which cannot be found by a deterministic evaluation. However a specific part of the operators manual to cope with initiating events in low power and shutdown operation should be available.

A level 2 PSA should be performed exemplary for one plant out of each PWR generation and BWR type of the NPPs operated in Germany. The PWR generations and BWR types are defined in the "Report for the Nuclear Safety Convention" (/NSK 98/). An actualization of the level 2 PSA in predetermined periods of time does not seem to be necessary, because new operational experiences generally will not significantly influence the results of the level 2 part of the PSA. If new insights on phenomena relevant for the plant response to a core melt accident become available, their influence on the results of the level 2 PSA should be investigated.

In this context it is again pointed out, that according to the state of the art a PSA should be used not primarily to characterize the safety status of a plant by one single probabilistic figure. The utility of a PSA lays mainly in the fact, that in a comprehensive ap-

proach nearly all safety relevant influences from design, construction, and operation are considered and thus weak points in the safety status of a plant can be identified and evaluated. By the present PSA, e.g., the low reliability of the manual cool down via the steam line safety valves – caused by the lack of criteria and insufficient training – and the missing precautions to prevent boron dilution during passive heat removal in shutdown operation have been found as weak points. Here it is especially important, that the PSA considers all safety functions which play a role for the deterministic safety design. If certain systems or measures are not considered in the PSA, because they are not required to meet, e.g., orientation values given in the PSA Guideline, weak points of these systems or measure cannot be detected by the PSA.

8.1.2.2 Extension of the available probabilistic methods

The investigations have shown, that the absolute frequency level of damage states is very low. As a consequence the relative importance of events which have been neglected up to now is increased. Mainly under this aspect the currently existing limitations of a level 2 PSA have the following importance in the view of GRS:

- The low frequencies of system and core damage states caused by internal initiating events make necessary the systematic consideration of the complete chain of anti-seismic design features (starting from a relevant spectrum of seismic effects at a NPP site different with respect to frequency, intensity, and dynamics, over the interaction between ground and buildings to the dynamic behavior of buildings and the resulting loads on structures and the operational and safety systems and their failure behavior). The effort for the practical application of the methods which are principally available is still unacceptably high.
- Although the estimated contributions to the frequency of damage states from the analyzed cable fire are negligible, a reliable investigation of fire induced failures in the I & C system requires a detailed consideration of failure causes (signal interruption, signal change, insertion of overvoltage) which could affect several redundancies
- The extremely low frequency of large releases of radionuclides during a severe accident could be considerably influenced also by very unlikely initiating events (mainly extreme flooding or extreme weather conditions or a large failure of vessels with high energy content).

- The decay heat removal by “counter current flow” is taken into account as safety function for the cooling of the reactor core. Mainly for this reason, the influence of the deborated condensate produced in the steam generator tubes on the criticality behavior of the reactor core has to be clarified. This question is especially important with respect to accidents with small primary system leak during power operation and to a total loss of the decay heat removal chains during mid loop operation in shutdown states.
- The utilities generally follow the concept to repair failed components also after accident initiation. This requires the consideration of such recovery measure in the PSAs.
- The considerable influence of low power and shutdown states on the frequency of damage states of the reactor core cooling shows the importance of a systematic investigation of the resulting influences on core damage accidents and the possible radionuclide releases in a level 2 PSA for low power and shutdown states.

8.2 Conclusions related to the safety of the reference plant

8.2.1 System and core damage states

The results of the level 1 part of the PSA allow the following statements and conclusions concerning the safety status of the reference plant:

- The absolute level of the damage state frequency is very low, in part the limits of a possible quantification are reached.
- Single component failures play a minor role – with the exception of cases with missing redundancy – due to high component reliability and high degree of redundancy.
- As an unavoidable consequence common cause failures are dominating – partially together with external events, which however can hardly be evaluated with the currently available methods.
- Further developments of methods are recommended in order to allow a quantification of actual contributions with low frequency and to allow a consideration or exclusion of potential contributions (common cause failures, external events, boron dilution).

8 Summarized evaluation and conclusions

- A modification of the system design is recommended with respect to identified weak points (e.g. redundant design of the decay heat removal chain), but first of all to reduce dominating contributions from common cause failures by diversity (mainly for the steam relief valves).
- Events during low power and shutdown operation contribute about 25 % to the frequency of systems damage states and therefore are not negligible, although up to now not all potentially relevant event sequences have been quantitatively evaluated. An extension of the low power and shutdown analysis into a level 2 PSA seems to be justified.

The PSA has shown the following possibilities to reduce the expected frequencies of system and core damage states:

- Reducing the frequency of small leaks can immediately reduce the frequency of core damage states.
- The protection goal oriented operators manual should be optimized, especially the transition from the event oriented part.
- By a modification of the emergency manual the full application of the potential of plant internal accident management also during LOCAs including steam generator tube ruptures should be made possible.
- The control of accidents during low power and shutdown operation can be improved by a specific operators manual.

8.2.2 Plant damage states

The total frequency of damage states is significantly lower than 10^{-5} per year. From the analysis of severe accidents starting during normal power operation the following conclusions are drawn:

- The accident analyses have shown, that even after a core meltdown a containment failure can be prevented also in the long-term. This requires however that the molten core can be kept inside the reactor pressure vessel. If the reactor pressure vessel is penetrated, the core debris in the long-term will get into the soil beneath the plant.

- With a probability of about 8 % a core meltdown will be followed by a large early radionuclide release, if the containment is damaged by a failure of the reactor pressure vessel under high system pressure or if the containment function is by-passed by a non-isolated steam generator tube rupture.
- With a probability of 15 % large early releases occur, if radionuclides reach the environment unfiltered via the annular room ventilation system, via a leak in steam generator tube which is covered by water, but cannot be isolated, or via the containment venting system with a damaged filter.
- With a probability of 48 % smaller amounts of radionuclides are released by filtered containment venting several days after accident initiation.
- The probability for a full function of the containment without the need for containment venting is about 31 %.
- The quoted probabilities are mean values of the calculated subjective probability distributions.

From the PSA results the following indications for a further reduction of the consequences of a core meltdown can be derived:

- The accident consequences can be reduced decisively, if the core debris can be retained inside the reactor pressure vessel.
- By cooling the containment atmosphere the pressure increase and thus the release of radionuclides can be limited.
- If the core debris can be hindered to intrude into the sump suction lines, a melt-through of the containment can be prevented.
- At least for existing plants it seems to be not feasible even with considerable additional effort, to absolutely prevent scenarios with large early release of radionuclides. Altogether the safety evaluation should be concentrated on the goal, to reduce the expected frequency of a core damage accident as far as possible, because in this way the overall accidental risk can be limited. Any core meltdown accident - even with intact containment – would have severe consequences.

8.3 General conclusions

From the investigations GRS draws the following general conclusions concerning the NPPs in Germany:

- The methods evaluated in the present PSA are qualified, to produce reliable results for a PSA up to level 2 for accidents during normal power operation. However, influences from external area events (like earthquake und airplane crash), from a large failure of vessels with high energy content, and from boron dilution events are not considered. For events during low power and shutdown operation a level 1 PSA can identify weak points of system design or of plant operation, with the same limitations as for a level 1 PSA for power operation. Additionally, recovery and measures of the plant internal accident management are not considered.
- Today the deterministic approach is not sufficient to perform a safety evaluation according to the state of the art. Supplementing probabilistic evaluations should be performed. At the current state of the methods a weak point analysis should be performed for low power and shutdown states.
- The results of a PSA, following the state of the art, are reliable, if the analysis is sufficiently detailed and appropriate data are used. The data base should be continuously adjusted with increasing operational experience.
- The low probabilities for large radionuclide releases following core meltdown accidents found in this PSA should be exemplary verified for the different PWR generations and BWR types (see /NSK 98/) of NPPs operated in Germany.
- Further probabilistic investigations should be concentrated on plant specific influences which are relevant for core meltdown accidents. The scope of the PSA should not be adjusted primarily to probabilistic orientation values – as quoted in the PSA Guideline -, but it should sufficiently consider all influences which could be relevant for the PSA results. Furthermore the available methods should be evaluated also for older BWR plants in Germany, which are different in important system features from those plants evaluated probabilistically in a comprehensive manner up to now.
- In order to come to an equally high quality of PSAs performed by various teams, requirements which are as far as possible unambiguous should be formulated, which can be applied in order to get a comprehensive PSA considering all relevant influences according to the state of the art,

- The performers of PSAs principally should have the possibility to use the pool of generic data available at GRS. However, the data sets actually used for a PSA should remain responsibility of the respective PSA team.

9 References

- /ALL 99/ Allelein, H.-J., Breest, A., Spengler, C.
Simulation of Core Melt Spreading with LAVA:
Theoretical Background and Status of Validation,
OECD Workshop on Ex-Vessel Debris Coolability, Karlsruhe, 1999
- /BEL 99/ Beliczey, S.
Quantifizierung von Leckhäufigkeiten an verschiedenen druckführenden
Systemen von Konvoi-Anlagen für unterschiedliche Betriebszustände
GRS Köln, Technische Notiz, Januar 1999
- /BER 98/ Berning, A., Faßmann, W., Preischl, W.
Technische, organisatorische und personenbezogene Anforderungen im
Rahmen des anlageninternen Notfallschutzes
BMU-1998-506, 1998, ISBN/ISSN 0724-3316
- /BRE 95/ Breitung, W., Redlinger, R.
A Model for Structural Response to Hydrogen Combustion Loads in Severe
Accidents
Nuclear Technology, Vol 111, Sep. 1995, pp 420-425
- /FAK 97/ Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraft-
werke
Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke,
Stand: Dezember 1996, BfS-KT 16/97, Juni 1997
- /FAK 97a/ Facharbeitskreis (FAK) Probabilistische Sicherheitsanalyse für Kernkraft-
werke
Daten zur Quantifizierung von Ereignisablaufdiagrammen und Fehlerbäu-
men
Stand: März 1997, BfS-KT 18/97, Juni 1997
- /FAR 97/ Farmer, M.T., et. al.
MACE Test M3b Data Report, Argonne National Laboratory,
MACE-TR-D13
Electric Power Research Institute, EPRI TR-108806, 1997

- /FAS 01/ Fasel, H.-J., Türschmann, M., Röwekamp, M.
Die Auswahl kritischer Brandbereiche bei probabilistischen Brandanalysen,
Technischer Bericht, GRS-A-2835, April 2001
- /GRS 90/ Gesellschaft für Reaktorsicherheit (GRS) mbH
Deutsche Risikostudie Kernkraftwerke Phase B
ISBN: 3-88585-809-6, 1990
- /GRS 93/ Kersting, E. et al.
Safety Analysis for Boiling Water Reactors,
A Summary, GRS-98, July 1993
- /GRS 98/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH
Untersuchungen der Sicherheitsreserven von Kernkraftwerken bei
auslegungsüberschreitenden Ereignisabläufen
GRS-A-2588, April 1998
- /GRS 01/ Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH
Probabilistische Sicherheitsbeurteilung bestehender Kernkraftwerke mit
Leichtwasserreaktor
GRS-A-Bericht, in Vorbereitung, 2001
- /HAI 01/ Haider, C. et al.
Erweiterte PSA der Stufe 1 im Hinblick auf die Behandlung übergreifender
Einwirkungen und die Berücksichtigung ihrer Unsicherheiten am Beispiel
einer Anlage vom Typ Konvoi
GRS-A-2836, August 2001
- /HÖR 89/ Hörtner, H.
Zum Nichtschließen der Erstabsperrramatur im Not- und Nachkühlsystem
im KWB A am 17.12.87, atw, Dezember 1989
- /HÖP 00/ Höppner, G.
PSA GKN 2: Feststellung der Wirksamkeitsbedingungen bei ATWS
GRS Garching, Technische Notiz TN-HOP-04/00, 1. September 2000

9 References

- /HOF 99/ Hofer, E.
On two-stage Bayesian modeling of initiating event frequencies and failure rates
Tecnote
Reliability Engineering and System Safety 66, 1999, S. 97-99
- /HOF 99a/ Hofer, E., Peschke, J.
Bayesian modeling of failure rates and initiating event frequencies
Proceedings of the European Conference on Safety and Reliability (ESREL), Munich Garching, Germany, 13.-17. September 1999
- /HOL 99/ Holtschmidt, H., et. al.
Untersuchungen der Sicherheitsreserven von Kernkraftwerken bei auslegungsüberschreitenden Ereignissen
GRS-A-2761, Dezember 1999
- /KEL 88/ Keller, W.
Stand und Bedeutung der Konvoi-Anlagen,
atw, August/September 1988
- /KLE 96/ Klein-Heßling, W., Arndt, S.
„RALOC MOD4 Cycle AE: Program Reference Manual“,
GRS Köln, 1996
- /KLO 99/ Kloos, M., Hofer, E.
SUSA: The PC Version of the Software System for Uncertainty and Sensitivity Analysis of Results from Computer Models User's Guide and Tutorial, Version 3.2,
GRS Garching, August 1999
- /KRE 97/ Kreuser, A., Peschke, J., Türschmann, M.
Erfassung und Bewertung von gemeinsam verursachten Ausfällen,
Abschlussbericht Teil 4,
Erweiterung und Nutzen einer generischen Wissensbasis zur Bearbeitung sicherheitstechnischer Fragestellungen bei Kernkraftwerken
GRS-A-2445, März 1997

- /KRE 98/ Kreuser, A., Peschke, J., Verstegen, C.
 Consideration of Interpretation Uncertainties in the Determination of Common Cause Failure Probabilities
 PSAM 4, New York, 1998
- /KRI 99/ Krieg, R., et. al.
 Reactor Pressure Vessel Head Loaded by a Corium Slug
 Vortrag, eingereicht zur 15. International Conference on Structural Mechanics in Reactor Technology (SMiRT), Seoul, August 1999
- /LÖF 00/ Löffler, H., et. al.
 Untersuchung auslegungsüberschreitender Anlagenzustände mittels Ereignisbaumtechnik am Beispiel einer Konvoi-Anlage
 GRS-A-2849, November 2000
- /MEI 01/ Meier, S.
 Ereignisbaum für Unfälle mit Leck in einer Anschlussleitung des RKL im Ringraum
 GRS Köln, Technische Notiz, MEI-TN-3/2001/-SR2306, 7.3.2001
- /NEA 00/ Nuclear Energy Agency, Committee on the Safety of Nuclear Installations
 International Common-Cause-Failure Data Exchange (ICDE) General Coding Guidelines
 ICDECG00, Revision 4, 19.10.2000
- /NRC 90/ U.S. Nuclear Regulatory Commission (USNRC)
 Severe Accident Risks:
 An Assessment for five U.S. Nuclear Power Plants
 NUREG-1150, December 1990
- /NRC 97/ U.S. Nuclear Regulatory Commission (USNRC)
 „MELCOR 1.8.4 - Reference Manual“,
 USA, Washington, July 1997

9 References

- /NRC 98/ U.S. Nuclear Regulatory Commission (USNRC)
Common-Cause-Failure Database and Analysis System:
Event Definition and Classification
NUREG/CR-6268, Vol. 2, June 1998
- /NSK 98/ Übereinkommen über nukleare Sicherheit -
Bericht der Regierung der Bundesrepublik Deutschland für die Erste
Überprüfungstagung im April 1999
Drucksache 13/11350, Bonn, August 1998
- /PIL 96/ Pilch, M., et. al.
Resolution of the Direct Containment Heating
Issue for All Westinghouse Plants With Large Dry Containments
or Subatmospheric Containments
NUREG/CR-6338, 1996
- /PRW 98/ Preischl, W., Berning, A., Faßmann, W., et. al.
Untersuchungen zu Handlungen des Betriebspersonals bei Notfallmaß-
nahmen
GRS-A-2617, Oktober 1998
- /PÜT 01/ Pütter, B.
PSA GKN 2: Thermohydraulische Untersuchungen zum Leistungsbetrieb
GRS-Arbeitsbericht, in Vorbereitung, 2001
- /SIE 98/ Siemens AG
Probabilistische Sicherheitsanalyse für das Gemeinschaftskernkraftwerk
Neckar, Block II
NDS4/09.98, September 1998
- /SON 99/ Sonnenkalb, M., et. al.
Untersuchungen von Maßnahmen des anlageninternen Notfallschutzes zur
Schadensbegrenzung für LWR - Zwischenbericht zum Vorhaben SR 2306
GRS-A-2735, November 1999

- /SON 01/ Sonnenkalb, M., et. al.
Untersuchungen von Maßnahmen des anlageninternen Notfallschutzes zur Schadensbegrenzung für LWR
Abschlussbericht SR 2306, GRS-Arbeitsbericht, in Vorbereitung, 2001
- /SWA 83/ Swain, A.D., Guttman, H.E.
Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications
NUREG/CR-1278, U.S. Regulatory Commission, August 1983
- /TIL 98/ Tiltmann, M., Rohde, J.
Wirksamkeit eines Systems katalytischer Rekombinatoren in Sicherheitsbehältern von DWR-Anlagen deutscher Bauart,
Schriftenreihe Reaktorsicherheit und Strahlenschutz, BMU-1999-538, 1999

List of figures

Fig. 3.1	Overview on GKN NPP units 1 and 2	8
Fig. 3.2	Functional scheme GKN 2	9
Fig. 3.3	Scheme of the principal safety installations of a PWR.....	10
Fig. 5.1	Contributions of event groups of initiating events to the total system damage frequencies and contributions of system function unavailabilities	103
Fig. 5.2	Contributions of the event groups of initiating events to the total core damage frequencies and contributions of unavailabilities of system functions.....	150
Fig. 5.3	Subjective probability distribution of the frequency of the event "system damage state" (only plant internal initiating events).....	163
Fig. 5.4	Core damage state frequency - uncertainties sorted by initiating events Fehler! Textmarke nicht definiert.	
Fig. 5.5	Core damage state frequency - uncertainties	172
Fig. 5.6	Subjective probability distribution of the annual event frequency of the event "core damage state" (only plant internal initiating events).....	173
Fig. 6.1	Pressure history in containment (SB), Annulus (RRu), service building (HAG) and environment, 10 cm ² leak at hot leg and failure of low pressure pumps, MELCOR 1.8.4	1
Fig. 6.2	Sum of produced and processed hydrogen and CO mass, 10 cm ² leak at hot leg and failure of low pressure pumps, MELCOR 1.8.4	1
Fig. 6.3	Pressure history inside containment and annulus, total station blackout and failure of surge line, MELCOR 1.8.4	186
Fig. 6.5	Principal set-up of the event tree.....	192
Fig. 6.6	Core melt in the lower part of the containment.....	206
Fig. 6.7	Load of sump suction pipe by core melt and fuel particles.....	208
Fig 6.8	Principal representation of the pressure evolution in the reactor coolant loop from core damage states until RPV failure	216

Fig. 6.9	Subjective probability distributions for the expected frequencies of the release categories.....	225
Fig. 7.1	Initiating Events Contributions of initiating events to the total frequencies of system damage states of the fuel element cooling Contributions of unavailabilities of system functions	287
Fig. 7.2	Initiating Events Contributions of initiating events to the total frequency of system damage states of fuel element cooling with closed/open RPV Contributions of system damage states from transients and LOCAs.....	288
Fig. 7.3	Initiating events Contributions of initiating events to the total frequencies of system damage states with closed reactor pressure vessel	289
Fig. 7.4	Initiating events Contributions of initiating events to the total frequency of system damage states with open reactor pressure vessel.....	290
Fig. 7.5	Initiating events Contributions of initiating events to the total frequencies of system damage states of deboration Contributions of the unavailabilities of system functions	291
Fig. 7.6	Uncertainties of the system damage state frequencies and of their total values.....	292

List of tables

Table 5.1	Initiating event frequencies	36
Table 5.2	Frequencies of triggering events and probabilities for the transition from triggering events to initiating events.....	38/ 39
Table 5.3	Relevant frequency intervals of the estimated triggering events.....	54
Table 5.4	Estimated frequencies of core damage states and release categories for those events which have not been analyzed in detail	63
Table 5.5	Probabilities of the transition from initiating events to system damage states.....	68
Table 5.6	Unavailabilities of system functions and the frequencies of system damage states of initiating events.....	70/71
Table 5.7	Core damage state attributes considered in level 2 of the PSA.....	112
Table 5.8	Summarized core damage states and correlation to the basic 35 core damage states for level 2 of the PSA.....	118
Table 5.9	Probabilities of the transition from system damages states to a restored safe state and to core damage states.....	121/123
Table 5.10	Unavailabilities of plant internal accident management and repair measures and the core damage frequencies of system damage states.....	123/125
Table 5.11	Probabilities of the transition from initiating events to core damage states.....	125/127
Table 5.12	Unavailabilities of system functions, plant internal accident management and repair measures and core damage frequencies for initiating events.....	127/129
Table 5.13	Probabilities of the transition from initiating events to core damage states with high, medium, low pressure	155
Table 5.14	Probabilities of the transition from initiating events to core damage states with availability of primary injection systems	155

Table 5.15	Probabilities of the transition from initiating events to core damage states for selected time periods.....	155
Table 5.16	Probabilities of transition from initiating events to core damage states due system function failures.....	156
Table 5.17	Fractiles, point values and mean values of the frequencies of system damage states sorted by initiating events.....	164
Table 5.18	Fractiles and mean values of the frequencies of initiating events.....	165
Table 5.19	Fractiles, point estimates and mean values of the transition probability from initiating event to system damage state.....	166
Table 5.20	Fractiles, point estimates and mean values of the core damage frequency sorted by initiating events.....	169
Table 5.21	Fractiles, point estimates and mean values of the transition probabilities from initiating events to core damage.....	170
Table 5.22	Fractiles, point estimates and mean values of the frequencies of core damage states.....	171
Table 6.1	Accident progression for a 10 cm ² hot leg leak and failure of low pressure emergency cooling.....	181
Table 6.2	Accident progression after transient with total loss of AC power and with consequential failure of surge line.....	184
Table 6.3	Branching points of the event tree.....	191
Table 6.4	Best-estimate values of the probability for the transition from core damage states to selected damage at the reactor cooling loop due to steam explosions in the lower plenum.....	199
Table 6.5	Best-estimate values of the probability of the transition from core damage states to hydrogen deflagrations or hydrogen detonations in selected compartments of the containment.....	202
Table 6.6	Examples of calculated states (pressure, temperature) of the containment atmosphere due to melt- and hydrogen ingress.....	204
Table 6.7	Probabilities for the erosion of the concrete foundation due to core melt.....	210

Table 6.8	Probability of the transition from core damage states to different final locations for core materials	214
Table 6.9	Probabilities of the transition from core damage states to the RPV pressure shortly before RPV failure for different initiating events	215
Table 6.10	Probabilities of the transition from core damage states to final states of the containment for different initiating events.....	218
Table 6.11	Probabilities of the transition from core damage states to release categories and uncertainty ranges for the frequencies of release categories.....	220/223
Table 6.12	Frequency of release categories and probabilities of the transition from core damage states to release categories	222/225
Table 7.1	Plant operational states of a 14-day standard outage of the reference plant	236
Table 7.2	Initiating events during low-power and shutdown operation	238
Table 7.3	Probabilities for initiating events (mean values) during the 14-day standard outage	242
Table 7.4	Expected values of the probabilities for triggering events per outage events and for the transition of triggering events to initiating events	246/249
Table 7.5	Mean values of the probabilities per outage of the transition from initiating events to system damage states and of the system damage states.....	255/259
Table 7.6	Mean values of unavailabilities of system functions and the probabilities of system damage states affecting fuel element cooling and of deborations after failure of residual heat removal per outage.....	261/265
Table 7.7	Fractiles, point values and mean values of the probabilities per outage of system damage states of fuel element cooling	293
Table 7.8	Fractiles, point values and mean values of the probabilities per outage of system damage states of deboration	294

**Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) mbH**

Schwertnergasse 1
50667 Köln
Telefon (02 21) 20 68 -0
Telefax (02 21) 20 68 -888

Forschungsinstitute
85748 Garching b. München
Telefon (0 89) 3 20 04 -0
Telefax (0 89) 3 20 04 -300

Kurfürstendamm 200
10719 Berlin
Telefon (0 30) 8 85 89 -0
Telefax (0 30) 8 85 89 -111

Theodor-Heuss-Straße 4
38122 Braunschweig
Telefon (05 31) 80 12 -0
Telefax (05 31) 80 12 -200

www.grs.de