BfS

SAFETY CODES AND GUIDES - TRANSLATIONS

Edition 08/97

Contents

Guides for the Periodic Safety Review of Nuclear Power Plants

- Basics of the Periodic Safety Review
- Safety Status Analysis
- Probabilistic Safety Analysis

of 18 August 1997

Leitfäden für die Periodische Sicherheitsüberprüfung für Kernkraftwerke

- Grundlagen zur Periodischen Sicherheitsüberprüfung
- Sicherheitsstatusanalyse
- Probabilistische Sicherheitsanalyse

vom 18. August 1997

Bundesamt für Strahlenschutz
Salzgitter

The German original of this translation was published in *Bundesanzeiger BAnz.* 1997, No. 232a.
In case of discrepancies the German text shall prevail.

Basics of the Periodic Safety Review
December 1996

Contents

1. Introduction

The nuclear power plants in the Federal Republic of Germany are subject to governmental supervision during construction, operation and decommissioning and in case of modifications of the plant and its operation mode if areas important to safety are concerned. During supervision, the plant conditions and its mode of operation are examined with regard to compliance with the regulations of the licensing decisions. Further, the necessity of the implementation of new safety-related knowledge resulting from operating experience, safety analyses as well as research and development is examined.

In the course of a longer lasting operating period, the range of knowledge to safety is broadened; the methods and instruments for safety analyses are being further developed. This should lead to a continued development of the plant's safety status and its operational safety. Thus, it is appropriate to perform an overall safety review for each operating nuclear power plant with light-water reactor at appropriate intervals. Accordingly, the Reactor Safety Commission (*Reaktor-Sicherheitskommission – RSK*) recommended a Periodic Safety Review (PSR) for the inspection of the current safety status of plants at its 238. meeting on 23 November 1988 (*Bundesanzeiger* 1989, No. 47a). An additional recommendation, which was issued at the 291. RSK-meeting on 17 May 1995 (*Bundesanzeiger* 1995, No. 158), putting the execution of the PSR in more concrete terms.

The PSR should be performed at intervals of about 10 years. It is provided that the RSK gives special attention to PSR results having general importance.

The licensee performs the PSR responding to his own responsibility for the safety of the plant. For some plants there are respective requirements stipulated in the licences.

The PSR supplements the information on the safety-related plant status for the governmental supervisory authorities. Planning and performance of the PSR are to be realised in co-operation between the licensee and the competent supervisory authority with orientation towards the guides of the PSR: " Basics of the Periodic Safety Review", "Safety Status Analysis", " Probabilistic Safety Analysis" and " Deterministic Analysis on Physical Protection".

Purpose of the guides is to stipulate a uniform procedure within the Federal Republic of Germany and to define a clear frame with regard to objective and scope of the PSR. These guides deal with the description of the plant's safety status by the licensee on the one hand, and the evaluation by the authorities with regard to §§ 17 and 19 of the Atomic Energy Act (*Atomgesetz - AtG*) on the other hand.

2. Objectives and principles of the periodic safety review

The necessary precautions to prevent damages according to the respective state of the art in science and technology have been demonstrated for the existing nuclear power plants by deterministic methods in the frame of the licensing procedure for granting the construction and operating licence pursuant to § 7 of the Atomic Energy Act.

The safety status of nuclear power plants should be determined in its entirety after a longer operating period and thus supplement the permanent review by governmental supervision of the operation. This shall be performed on the basis of licences granted, the actual condition of the existing plant and the requirements of the state of the art in science and technology. The results shall be evaluated according to §§ 17 and 19 of the Atomic Energy Act. The performance of the PSR and the evaluation of results is to be carried out by application of deterministic and probabilistic methods.

The defense-in-depth concept for nuclear power plants comprises four safety levels (Fig. 1). On each level within this safety concept, technical systems and preventive measures for anticipated operational occurrences and accidents as well as measures for bringing them under control up to the limitation of consequences of beyond-design-basis event sequences are assigned to the respective plant conditions. The technical systems and measures at the different levels have to be effective independently of failure or loss of the precedent function and cover the events not kept under control on the respective lower level. This is to maintain the integrity of the sequential barriers against release of radioactive material within the plant and into the environment and thus ensuring the protection against ionising radiation during the operation of nuclear power plants.

The functions of technical systems and measures related to the respective precautions of level 1 "normal operation" and level 2 "abnormal operation" are designed to prevent failures during normal operation and to bring anticipated operational occurrences under control respectively in order to prevent an accident at the plant. Within the scope of the PSR, it is to be demonstrated at these levels to which extent the requirements stipulated are met and in which way the technical systems and measures have proved their reliability during operation so far by evaluation of operating experience taking into account safety-relevant areas of operational management.

On the third safety level, the "accident level (design basis accidents-DBA)", the safety system of the plant has to control a broad spectrum of DBAs in a reliable and effective way. The radiological planning values for DBAs pursuant to § 28 para. (3) of the Radiation Protection Ordinance (*Strahlenschutzverordnung - StrlSchV*) are not to be exceeded. The PSR should be focused on the "accident level". The central question is

to which extent the postulated accidents can be controlled with appropriate efficiency and reliability by the precautions provided.
Measures for special, very rare events and hypothetically postulated beyond-design-basis plant conditions are assigned to the 4th safety level for which radiological planning values do not apply.
For special, very rare events, the strain of specified systems and components is to be limited, specified stresses have to be endured and transfer of the plant into a safe state has to be made feasible. This also implies events where in the case of more recent plants specific precautionary measures due to special design requirements are taken (e. g. aircraft crash). As far as there are non-compliances at older plants, it is to be described within the scope of the PSR with the aid of a probabilistic approach to what extent this implies a risk relevance or an imbalance of the plant's safety concept.*) Whether any additional precautions are to be taken for these reasons, also has to be stated considering the principle of commensureability.

In case of beyond-design-basis plant conditions, which may result from accidents with additional system failures not considered in the design, severe accident management measures shall serve to prevent severe core damage or to reduce radiological consequences. Within the scope of the PSR, it should be demonstrated which measures are provided against beyond-design-basis events. Further, it should be documented to what extent effective safety precautions, which are technically reasonable within the scope of the plant's safety concept, have been provided in addition to the existing precautions.
The deterministic review of a plant is to be based on protection goal oriented requirements and conditions to be met by the plant within the scope of a PSR (see section 4.2) for a generic spectrum (reference list) of accidents to be considered, special, very rare events and beyond-design-basis plant conditions.
The examination of the balance of the safety concept of the entire plant and the determination of the total frequency of not-controlled plant conditions are performed by a probabilistic safety analysis (PSA). Further, the status of physical protection of the plant is to be described

<table>
<tr><th>Safety Levels</th><th colspan="2">Precautionary Areas / Radiation Protection Requirements</th><th colspan="2">Plant States / Events</th><th>Frequencies of Plant States / Events</th><th colspan="2">Technical Systems and Measures</th><th>Design Principles</th></tr>
<tr><td>1</td><td rowspan="4">Necessary Precaution to Prevent Damages According to the Atomic Energy Act</td><td rowspan="2">§ 45 Radiation Protection Ordinance

§ 45 StrlSchV</td><td rowspan="2">Operating Conditions</td><td>Normal Operation</td><td>regularly</td><td rowspan="2">Operational System</td><td>Operational Components and Systems</td><td>- Conservative Design
- Basic Safety
- Quality Assurance
- Monitoring
- Personnel Qualification</td></tr>
<tr><td>2</td><td>Abnormal Operation</td><td>often</td><td>Control and Limiting Equipment, Equipment Protection</td><td>and additionally:
- Inherent Safety
- Thermohydraulic and Reactor-physical Stability</td></tr>
<tr><td>3</td><td>§ 28 (3) Radiation Protection Ordinance

§ 28 (3) StrlSchV</td><td colspan="2">Design-Basis Accidents</td><td>rare</td><td colspan="2">Safety Systems</td><td>and additionally:
- Redundancy
- Diversity
- Fail Safe
- Physical Separation and Partitioning
- Automatisation
- Self-Sufficiency</td></tr>
<tr><td rowspan="2">4</td><td rowspan="2">Limitation of Radiation Exposure, No Quantified Radiation Protection Requirements</td><td rowspan="3">Severe Accidents</td><td>Special, Very Rare Events</td><td rowspan="2">very rare</td><td colspan="2">Sepcific Precautionary Measures</td><td>Specific Design Requirements</td></tr>
<tr><td>Beyond-Design-Basis Plant Conditions</td><td colspan="2">On-site Severe Accident Management</td><td>- Flexible Utilisation of Existing Systems
- Engineering Practice at Emergency Protective Equipment</td></tr>
<tr><td colspan="2">Residual Risk</td><td>Damage States with Significant Impact on the Environment</td><td>extremely rare practically excluded</td><td colspan="2">Off-site Emergency Management and Disaster Control</td><td>Off-site Emergency Management and Disaster Control</td></tr>
</table>

Fig 1: Safety Concept for Nuclear Power Plants

*) Explanation of terms in Appendix A

3. Legal classification of PSR and implementation of results

The PSR supplements the permanent review of nuclear power plants within the scope of governmental supervision.

The PSR is performed by the licensee in response to his own responsibility for the plant's safety and, corresponding conditions included in the licences of some plants. There is no direct legal obligation to perform a PSR.

In current practice, the concrete procedure for the PSR performance is regularly agreed between the licensee and the supervisory authority.

The implementation of the PSR results is oriented to the general regulations, i. e. the instruments of the Atomic Energy Act.

4. Scope and parts of PSR

The documentation of a plant's safety status within the scope of the PSR comprises the results of the following parts:

- the deterministic safety status analysis in form of a protection goal oriented review of the plant's safety status including a description of the operational management and evaluation of operating experience,
- a probabilistic safety analysis,
- a review of the plant's physical protection concept.

The individual parts of the PSR require different approaches, but they are related to each other with regard to a proper overall assessment of the plant. Interactions and linkages result particularly from the probabilistic and deterministic aspects complementing one another regarding the protection goal oriented review of the plant's safety status. Therefore, it is appropriate to work out the parts within the same period.

The following sections explain the relevant steps and contents of the aforementioned parts. A scheme of the PSR is given in Fig. 2.

In view of an effective and expedient performance of the PSR, the procedure should be stipulated in agreement between licensee, authority and experts consulted on the basis of the present guides for the PSR. For this purpose, a concrete frame for the scope of the PSR and the following review as well as for the schedule should be agreed upon.

In order to simplify the performance of each further PSR and to keep the efforts reasonable, subsequent PSRs can be performed as Delta-PSRs based on the results of the respective previous PSR and the existing PSR documentation can be continued.

4.1 Current plant description

The analyses of the different parts of the PSR have to be preceded by a plant description. The plant description serves the purpose of giving an up-to-date survey of the safety concept, the plant's design features and of all substantial measures important to safety.

The description of the plant and of the structures, systems and equipment important to safety has to contain relevant information on the following aspects:

- task and safety function, respectively,
- configuration, arrangement, and design.

An outline of the structure for the plant description is given in Appendix B.

The plant description is to contain backfittings and major modifications important to safety of the plant after start-up or the last PSR. Further, backfitting measures and severe accident management measures which have not been implemented yet, can be included if they are licensed or if a license has been applied for and if they are examinable. The concept of severe accident management should be specified in a separate chapter (see section 4.2). In-depth system descriptions, which are required for the analyses (Safety Status Analysis, PSA), are to be given where it is appropriate in the analyses.

A description of physical protection features and safeguard measures is part of the "Deterministic Analysis on Physical Protection" (see section 4.4).

4.2 Deterministic safety status analysis

The deterministic safety status analysis should be performed according to the procedure stated in the guide "Safety Status Analysis"

According to this guide, the procedure is provided as follows:

- a deterministic review of engineered safety features of the plant according to the protection goal oriented requirements of nuclear regulations [*)] and the accident spectrum to be considered,
- description of the equipment and measures for special, very rare events as well as of the severe accident management concept,
- description of operational management and evaluation of operating experience.

The deterministic protection goal oriented review concentrates on the description how the analysed accidents are controlled by the plant's engineered safety features. The actual condition of the systems important to safety is to be examined with regard to the availability of required safety functions for accident control with sufficient efficiency and reliability and therewith that the safety criteria for nuclear power plants (*Bundesanzeiger* 1977, No. 206) based on the protection goals

- reactivity control,
- cooling of fuel elements,
- confinement of radioactive material and
- limitation of radiation exposure.

are met according to the state of the art in science and technology.

On safety level 3, the deterministic analyses of systems and measures important to safety are to be based on requirements oriented towards protection goals, also considering necessary requirements of safety levels 1 and 2, as e. g. with regard to the quality condition.

The protection goal oriented requirements are based on the sublegal nuclear regulations. They also consider more recent, corroborated findings and are ordered hierarchically according to the above-mentioned protection goals in order to ensure a uniform application of fundamental requirements, irrespective of specified technical solutions, within the performance of the safety status analysis.

The protection goals are deemed to be fulfilled if the protection goal oriented requirements, particularly the necessary safety functions, are met. In this respect, technical design not complying literally nuclear regulations is permissible, too.

The guide "Safety Status Analysis" includes a reference list of accidents to be considered for the specification of the plant-specific accident spectrum; plant-specific boundary conditions are to be taken into consideration.

[*)] Explanation of terms in Appendix A

The review of engineered safety features should be based on valid documentation and verifications. Additional analyses are to be performed particularly if there are doubts about their validity or if required from a probabilistic point of view (risk relevance) and under consideration of particular plant conditions.

If it should be found that particular safety functions are not available at all or not available with the required efficiency and reliability, a final safety assessment considering the results from the other parts of the PSR is to be performed (see section 5.1).

The efficiency of equipment and measures for special, very rare events is to be stated in the scope of safety level 4 using engineering-related assessments and plausibility considerations including probabilistic estimations.

The special, very rare events to be considered are stated in a reference list included in the guide "Safety Status Analysis"; plant-specific boundary conditions are to be taken into consideration.

In addition, the measures stated in the plant's (severe) accident management manual are to be presented in a separate chapter. The implemented on-site accident management measures are to be presented with reference to the beyond-design-basis plant conditions stipulated in the guide "Safety Status Analysis". The existing documents and verifications are to be used for this presentation.

The description of operational management and evaluation of operating experience is an additional essential part of the safety status analysis. Essential subjects are: technical knowledge and operational organisation, periodic testing and in-service inspections, maintenance, experience feedback, radiation protection and emergency preparedness. The evaluation of operating experience is to concentrate on safety aspects of normal operation, anticipated operational occurrences and accidents to be considered. The results are to be judged with regard to operating experience important to safety of plant equipment. Assessment of the results is to demonstrate whether the systems engineering requirements stated for levels 1 and 2 of the safety concept are met, and whether reliable operation with regard to accident prevention is ensured and can also be expected for the future.

PERIODIC SAFETY REVIEW FOR NUCLEAR POWER PLANTS (PSR)

<table>
<tr><td>PARTS</td><td colspan="2">Safety Status Analysis</td><td>Probabilistic Safety Analysis (PSA)</td><td>Physical Protection</td></tr>
<tr><td>STANDARDS</td><td colspan="2">Guide
Safety State Analysis</td><td>Guide
Probabilistic Safety Analysis</td><td>Guide
Deterministic Analysis of the Physical Protection</td></tr>
<tr><td colspan="5">Agreement on PSR Procedure between Licensee and Authority</td></tr>
<tr><td rowspan="4">PROCEEDING OF THE LICENSEE</td><td colspan="3">Current Plant Description</td><td></td></tr>
<tr><td>Assessment of the Plant´s Safety Systems according to the Requirements and Standards of the Protection Goal Concept</td><td>Description of Operational Management and Evaluation of Operating Experience</td><td rowspan="2">Examination of the Balance of the Safety Concept and Determination of Cumulative Frequency of not Controlled Plant States by Probabilistic Methods

Report: PSA</td><td rowspan="3">Report:
State of Physical Protection</td></tr>
<tr><td>Report:
Deterministic Protection Goal Oriented Review</td><td>Report:
Operational Management and Operating Experience</td></tr>
<tr><td colspan="3">Report: Final Review of the Safety Status involving the Respective Results of the Parts of the PSR</td></tr>
<tr><td rowspan="2">PROCEEDING OF THE AUTHORITY</td><td colspan="2">Protection Goal Oriented Evaluation, if necessary, with Consultation of external Experts</td><td>Evaluation, if necessary, with Consultation of external Experts</td><td>Evaluation, if necessary, with Consultation of external Experts</td></tr>
<tr><td colspan="4">Overall Assessment by the Supervisory Authority, Administrative Measures and Directives</td></tr>
</table>

Fig. 2:Survey of the Periodic Safety Review (PSR) System

4.3 Probabilistic safety analysis

Kind and scope of the probabilistic safety analysis to be performed are stated in the "PSA-Guide".

The results of the PSA are to supplement the deterministic assessment of the plant's safety status and its operational safety and be referred to for the determination of the necessity and urgency of safety improvements (see chapter 5). Vulnerabilities can be detected by a comparison of individual frequencies of not controlled plant conditions. Further, the balance of the safety concept of the plant can be assessed in this way.

4.4 Physical protection

Kind and scope of the physical protection of the plant is stipulated in the guide "Deterministic Analysis on Physical Protection".

4.5 In-depth analyses of individual aspects

Purpose of the present "Basics of the Periodic Safety Review for Nuclear Power Plants", i. e. definition of a clear frame with regard to objective and scope of the PSR, takes up the legal criteria of damage precaution according to the state of the art in science and technology. The efforts for creating a practicable and appropriate frame for the PSR are based on the legal requirements of safety precautions.

The guides specify comprehensively requirements and procedures which can be regarded as practicable and feasible.

Analyses of scenarios and event sequences, i. e.
- fire scenarios,
- plant conditions with less than nominal power,
  - start-up and shutdown operation,
  - partial-load operation,
- standstill operation,
- human actions during respective operational states and event sequences

which already have been taken into consideration in part nationally and internationally by the use of generally accepted methodologies, are not to be excluded by the present guides. *) However, it is useful to perform analyses not specified by the present guides separately with regard to contents and procedure, as far as it seems to be necessary in the particular case.

If in-depth analyses are required for individual aspects exceeding the frame provided by the PSR, they should be excluded from the PSR-procedure and reviewed in the course of the permanent supervision process.

*) In the course of drafting the PSA-guide, it had been considered at that time (1990) that in addition to the analysis of initiating events during full-power operation it should be examined qualitatively or by course analyses to what extent events during plant conditions with less than nominal power may lead to special requirements, If necessary , additional in-depth analyses would have to be performed for other plant conditions, as e. g. for zero power, operation to remove residual-heat, partial load, operational test, operation with reduced availability of operational systems (abnormal operation), start-up and shutdown and maintenance outage.

5. Results of the PSR

5.1 Final review and documentation by the licensee

At the end of a PSR, the licensee should review the safety status of the plant. For this purpose, the results of the respective analyses have to be summarised for a substantial overall picture. In the case of plants not built literally pursuant to present nuclear regulations, it has to be assessed to what extent the protection goals stipulated in the nuclear regulations have been met and to what extent the safety concept is well balanced. The review may include planned improvements important to safety.

The individual analyses and results should be summarised and submitted to the competent supervisory authority as documentation for the PSR.

The contents of the reports should be verifiable; the documents used have to be stated.

The reports may be structured as follows:
- Current plant description,
- Report: Deterministic protection goal oriented review,
- Report: Operational management and operating experience,
- Report: Probabilistic safety analysis,
- Report: Status of physical protection,
- Report: Final review of the safety status involving the respective results of the parts of the PSR.

5.2 Assessment of the PSR-results by the nuclear supervisory authority

The nuclear supervisory authority assesses the documentation of the safety status of the plant submitted for the PSR with regard to §§ 17 and 19 of the Atomic Energy Act. The experts consulted by the authority examine the submitted PSR. The methods for the individual parts described in the PSR-guides should be used as a basis for the examination.

Results from the parts of the PSR (Safety Status Analysis and Probabilistic Safety Analysis) which do not comply with the protection goal oriented requirements or reliability requirements of engineered safety features, have to be subdivided into deviations not important to safety and important to safety requiring corrective measures as a part of the overall assessment.

The assessment of the safety significance of the results should be performed according to the following criteria:
- does the evaluation of operating experience confirm sufficient reliability of the respective system,
- are the accidents to be considered which cover all plant conditions controlled by the existing engineered safety features according to the protection goal oriented requirements with the required efficiency and reliability,
- are there technical equipment and measures for beyond-design-basis plant conditions,
- were vulnerabilities and/or imbalances within the safety concept identified.

If there are deviations important to safety which require corrective measures, the results of the PSA can also be used for the assessment of urgency of the measures. These measures have to be taken in such a way that there are no more deviations important to safety after their implementation.

The measures to be taken and directives to be given by the responsible supervisory authority in the scope of the overall assessment of the results are established according to the principle of commensureability.

Appendix A

Explanation of terms used in the scope of the PSR

Nuclear Regulations

The term nuclear regulations comprises the entirety of all sublegal plant requirements important to safety according to the state of the art in science and technology including more recent, corroborated findings. These requirements are stipulated in the documents listed below:

- safety criteria for nuclear power plants,
- guidances of the Reactor Safety Commission (RSK-Leitlinien) for pressurised water reactors,
- accident guidances for pressurised water reactors,
- guidelines of the Federal Committee for Nuclear Energy
- safety standards of the Nuclear Standards Committee (KTA-Regeln),
- recommendations of the Reactor Safety Commission and the Commission on Radiological Protection.

Balance of the safety concept

The safety concept shall be considered well balanced if the individual contributions (such as frequencies of hazard states for initiating events or for event sequence paths) do not dominate the respective result.

Hazard state

Plant condition where the protection goals, such as the confinement of radioactive material, cooling of fuel elements, are no longer under the control of the systems designed for this purpose. Without further measures, a damage state can arise. It is possible that a hazard state can be transferred into a safe plant condition by means of severe accident management measures and that a damage state can thus be prevented.

Damage state

Plant condition from which a loss of barriers can develop so that the confinement of radioactive material is no longer guaranteed. This can be: core damage, severe core damage, core meltdown or larger damage to fuel elements outside the reactor core (e.g. in the spent fuel pool). Severe accident management measures can be considered to keep radiological damage inside and outside the plant as low as possible.

Containment envelope

The containment envelope is the system consisting of containment vessel and the surrounding building as well as auxiliary systems to retain and filter possible leakages from the containment vessel.

Initiating event

Disturbances and damages to components and parts of the plant initiating an actuation of the safety systems are called "initiating events".

Plant-specific reliability parameters

Parameters which are employed to determine the reliability of components or systems (failure rates, failure probabilities) are called reliability parameters. Plant-specific reliability parameters are parameters based on data and information from the plant which have to be recorded in an appropriate way. To estimate the plant-specific reliability parameters, generic advance information is generally to be taken into account in an adequate way (Bayes` Methodology).

Safety system

The safety system is the entirety of all systems of a reactor plant having the task of protecting the plant against unpermissible stress and, if accidents should occur, of keeping their effects on the operating personnel, the plant and its environment within the preset limits.

Operational system

The operational system comprises all the systems, circuits and auxiliary systems which are exclusively required for the normal operation including anticipated operational occurrences. These have to be designed in such a way that accidents as a consequence of abnormal operational conditions are prevented with sufficient reliability.

Appendix B

Outline for the plant description

1 Constructional facilities

1.1 General layout and basic design

- Reactor Building,
- Reactor Auxiliary Building,
- Turbine Building,
- Switchgear Building,
- Emergency Diesel Building,
- Emergency Feedwater Building (PWR),
- Independent Emergency Building (BWR),
- Structures for Cooling Water,
- Other Constructional Facilities.

2 Systems and facilities

2.1 Reactor coolant system

- Reactor Pressure Vessel,
- Pressure Boundary,
- Reactor Core,
- Reactor Pressure Vessel Internals,
- Reactor Coolant Pumps/Coolant Circulating Pumps,
- Pressurising System (PWR),
- Steam Generators (PWR).

2.2 Reactor auxiliary systems

- Volumetric Control System (PWR),
- Chemical Injection System (PWR),
- Coolant Purification System (PWR),
- System for Coolant Storage (PWR),
- Reactor Water Purification System (BWR),
- Safety Cooling Systems,
- Emergency Feedwater System (PWR),
- System for Automatic Depressurisation/Pressure Limitation (BWR),
- Systems for Handling and Storage of Fuel Elements and Reactor Components,
- Spent Fuel Pool Cooling and Purification System,
- Nuclear Sampling System,
- Reactor Scram System,
- Ventilation Systems.

2.3 Containment envelope

- Reactor Containment Vessel,
- Containment Isolation/Penetration Isolation,
- Pressure Suppression System (BWR).

2.4 Steam and power conversion system

- Main Steam System,
- Steam Turbine Generator Set,
- Condensing System,
- Feedwater System.

2.5 Cooling water systems

2.6 Auxiliary systems

- Blow-down Water Treatment Installation,
- Condensate Purification System (BWR),
- Air Compressors,
- Demineralisation System,
- Auxiliary Steam System.

2.7 Electric plant equipment

- Power Supply,
- Auxiliary Power Supply,
- Emergency Power Supply,
- Battery System,
- Monitoring of Power Installations,
- Earthing and Lightning Protection Installations.

2.8 Control room, alarm system, instrumentation

- Main Control Room and Auxiliary Control Panels,
- Remote Shutdown Station,
- Process Computer System,
- Accident Instrumentation,
- Reactor Protection System including Safety Instrumentation and Control.

2.9 Radiation protection

2.10 Fire protection

Guide Safety Status Analysis
December 1996

Contents

1 Introduction

The description of the safety status of a plant in the course of a periodic safety review (PSR) shall comprise the results of a deterministic safety status analysis, a probabilistic safety analysis (PSA) as well as a description of the plant´s physical protection concept as parts of PSR.

In the course of the safety status analysis, the licensee should perform a deterministic protection goal oriented review of the existing engineered safety features of the plant, describe operational management and evaluate safety-related operating experience.

The present guide "Safety Status Analysis" including its appendices further specifies the objective, the procedure and the degree of details of the review for performing the safety status analysis.

The specifications of this guide should be applied to the performance of safety status analyses in all nuclear power plants with light water reactors in operation in the Federal Republic of Germany.

2 Objective of the safety status analysis

It is the objective of the safety status analysis to review the system functions of all systems important to safety of a nuclear power plant in a deterministic way.

It is to be determined here, if and to what extent
- protection goals are met by engineered safety features of the plant (deterministic, protection goal oriented review),
- plant technology has proven by operating experience, also with respect to a future, safe operation (operational management and operating experience).

During the deterministic, protection goal oriented review should be examined how the protection goal oriented requirements of the nuclear regulations*) are met. This should be performed on the basis of a detailed description of the current status of systems important to safety and equipment of the plant as well as the loads to be expected according to the accidents to be considered.

Description of operational management and evaluation of operating experiences acquired over a longer operational period constitutes part of the safety status analysis and should supplement and ensure the results of the deterministic review.

The results of the safety status analysis are to represent the basis for the final safety assessment of the plant to be reviewed as described in Section 5.1 of the „Basics of the PSR for Nuclear Power Plants“.

3 Protection goal oriented requirements and specifications for the safety status analysis

Requirements and specifications related to the deterministic safety status analysis of a plant are composed of:
- the protection goal oriented requirements of the nuclear regulations,
- the generic spectrum (reference list) of accidents to be taken into account,
- specifications to describe the equipment and measures for special, very rare events as well as accident management.

The deterministic review of the safety status of a plant is to be performed in a protection goal oriented way. This means that the existing nuclear regulations are applied in such a way that the keeping of fundamental protection goals is reviewed.

All safety-related requirements to be met by the plant in order to fulfil the protection goals:
- reactivity control
- cooling of fuel elements
- confinement of radioactive material and
- limitation of radiation exposure

based on the safety criteria for nuclear power plants are summarized in the protection goal oriented structure of the nuclear regulations (cf. Section 3.2). They refer to safety-related systems and measures as well as systems with safety functions (engineered safety features) on the individual safety levels of the safety concept for nuclear power plants and are based on the nuclear regulations.

3.1 Spectrum of accidents to be considered, special, very rare events and beyond-design-basis plant conditions

Appendix A comprises a reference list of accidents to be considered, special, very rare events (ATWS and severe civil impacts for which specific precautionary measures are to be taken) as well as beyond-design-basis plant conditions for pressurised as well as for boiling water reactors.

Starting from this generic spectrum, a plant-specific spectrum shall be derived for performing the review. If, taking into consideration the special plant conditions and the accidents dealt with in the licensing and supervisory procedure, it seems appropriate from a probabilistic perspective (risk relevance), further events are to be included into the review.

Such a plant-specific list should cover the entirety of events with safety-endangering loads for the plant. It is expedient that the required agreement between the licensee and the authorities takes place at the beginning of the safety status analysis.

3.2 Protection goal oriented structure of the nuclear regulations

The nuclear regulations reflect the development of technical experiences with design, construction and operation of nuclear power plants and, in addition to requirements significant for technical safety, also describe the execution of individual technical solutions. The protection goal oriented structure of the requirements set by the regulations is to ensure with regard to the performance of the safety status analysis a uniform application of the fundamental requirements of the nuclear regulations, independent of individual technical solutions, and including more recent, corroborated findings.

The literal application of the presently existing nuclear regulations to plants and/or parts of the plant built according to specifications of regulations applicable at that time is not expedient. For this reason, the requirements of the PSR were extracted from the nuclear regulations and assigned to the protection goal structure. This structure provides a hierarchical structure of fundamental, technical safety criteria and requirements as well as detailed technical realization regulations.

The protection goal oriented requirements predominantly relate to level 3 of the safety concept for nuclear power plants, considering necessary requirements of levels 1 and 2, like e.g. the quality status of safety-related parts of the plant.

The hierarchical structure of these requirements to be met by nuclear power plants with pressurised water reactors and boiling water reactors consists of four levels:
Level I safety objective,
Level II protection goals,
Level III safety functions,
Level IV measures for ensuring the safety functions (examples for good practice).

Fig. 1 shows the scheme of the protection goal oriented structure of the nuclear regulations.

Appendix B of the guide provides an outline of the fundamental protection goal related requirements and fundamental requirementsregarding support functions common to all protection goals.

The protection goal oriented structure of the nuclear regulations is mainly applied in accident analyses for the deterministic review of engineered safety features of the plant (cf. Section 4.1.3).

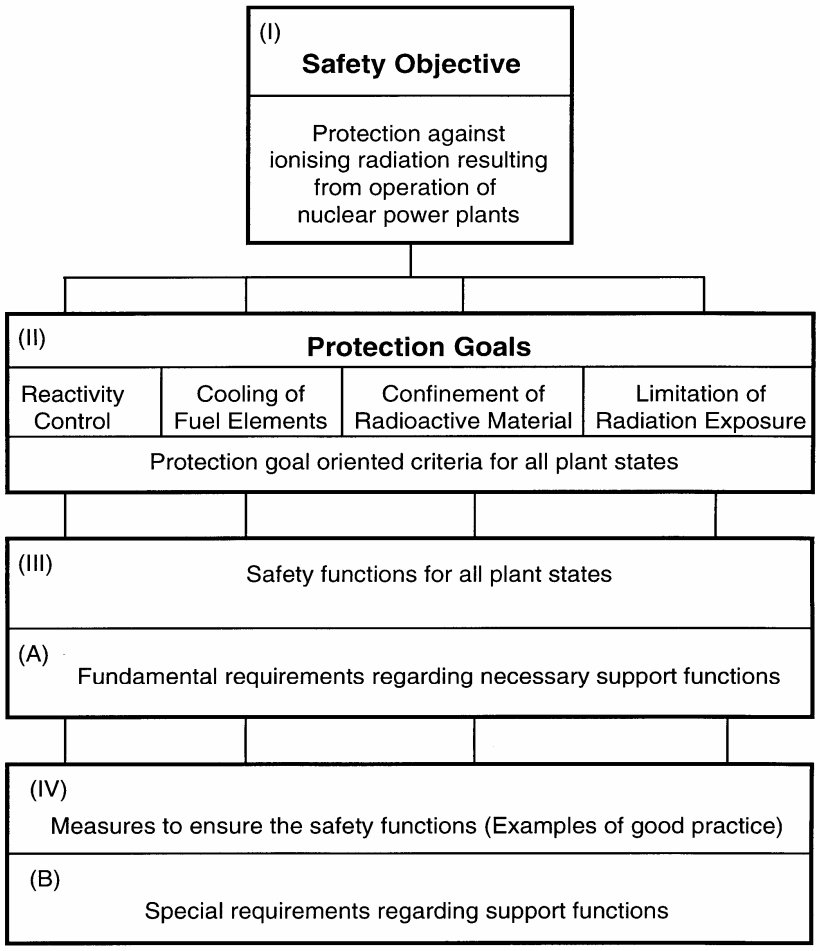

Fig. 1: Scheme of the protection goal oriented structure of the requirements of the nuclear regulations

4. Partial areas of and procedure in safety status analysis

The safety status analysis comprises the partial areas
- deterministic, protection goal oriented review and
- description of the equipment and measures for special, very rare events as well as severe accident management,
- description of operational management and evaluation of operating experience.

The description of safety-related areas of operational management and evaluation of cumulated operating experiences over a longer operational period constitute part of the safety status analysis and are to supplement and verify the results of the deterministic review.

The performance of the partial areas of the safety status analysis and the results as well as the representation of operational management and evaluation of operating experience are to be documented in separate reports.

Fig. 2 shows a flow chart on the procedure of the deterministic safety status analysis.

4.1 Deterministic, protection goal oriented review of engineered safety features

The deterministic, protection goal oriented review of the safety status of the plant comprises:
- the detailed description of the current status of engineered safety features (system descriptions),
- a description of safety-related areas reaching beyond plant or system level,
- a review of whether the protection goal oriented requirements for the accident spectrum under consideration are met by the systems (protection goal oriented review of the systems).

Contents and scope of the deterministic protection goal oriented review in the course of the safety status analysis are oriented at events according to the accident spectrum to be considered and the requirements of the individual levels of the safety concept of nuclear power plants to be met by safety-related parts of the plant.

For normal operation (safety levels 1 and 2), the requirements relate to reliable avoidance of accidents. It shall to be shown by evaluating operating experience that no indications for an inadmissible increase of

susceptibility to accidents can be perceived which were not worked against (cf. Section 4.2)

On the accident level (safety level 3), it has to be demonstrated on the basis of valid verifications that the accidents to be covered are controlled and that the safety objectives are thus observed. The main emphasis of the deterministic protection goal oriented review should concentrate on this area.

4.1.1 Description of the current status of engineered safety features (system descriptions)

As far as necessary for the review of systems, detailed descriptions of active and passive engineered safety features shall be provided. In particular such information (cf. Appendix C) like:

- functions of the system,
- system structure and spatial arrangement,
- operating modes of the system,
- design,
- functional testing of the system and status of quality

may be taken into consideration.

4.1.2 Plant and system-interfacing areas

In addition to the description of active and passive engineered safety features, safety-related areas concerning several parts of the plant or the entire plant are to be described, namely:

- accident instrumentation/accident resistance,
- radiation protection and activity monitoring,
- protection against internal impacts,
- protection against external impacts,
- annunciation and monitoring system,
- waste management.

Safety related technical systems and measures significant in these areas are to be described.

4.1.3 Accident analysis and protection goal oriented review of the systems

With in the accident analysis and protection goal oriented review of the systems it should be examined to which extent relevant safety functions are available and effective in the form of engineered safety features for sufficient control of the respective accident under consideration.

The source of verifications for accident control (sequence analyses) existing from licensing and supervisory procedures should generally be used. New analyses are normally required if only there are justified doubts with respect to the corraborated statements or the conservativeness of existing verifications. These supplementary analyses can be performed using realistic initial and boundary conditions (best-estimate procedures) and considering operating experience.

In case of new analyses of accidents of the predetermined accident spectrum (cf. Section 3.1), a sequence description is to be presented. The loads and effects on the plant and the environment to be expected are to be described for the respective accident scenario qualitatively and quantitatively, and the essential boundary conditions on which the accident analysis is based are to be presented.

The requirements of the protection goal oriented structure of the nuclear regulations (Appendix B) provide the comparative parameter for the review of the systems. The necessary safety functions and the deterministic requirements to be met by effectiveness and reliability of the systems are stated there (cf. Section 3.2).

The essential principle in the review of the systems is the protection goal oriented procedure. A formal comparison with the requirements of the regulations, especially with respect to the technical realisation, is not expedient for older plants.

Generally, accident control is demonstrated when, upon review of the systems, the criteria in level II related to the protection goals and the safety functions of level III (according to the structure explained in Section 3.2) are met .

The individual technical solutions of level IV are to be regarded as exemplary solutions. Other measures herefor are possible, but it has to be shown that the safety functions required according to level III are met. A respective procedure also applies to requirements regarding support functions common to all protection goals.

The results of the deterministic system review can show deviations compared to the protection goal oriented requirements to be met by the engineered safety features (cf. Section 5).

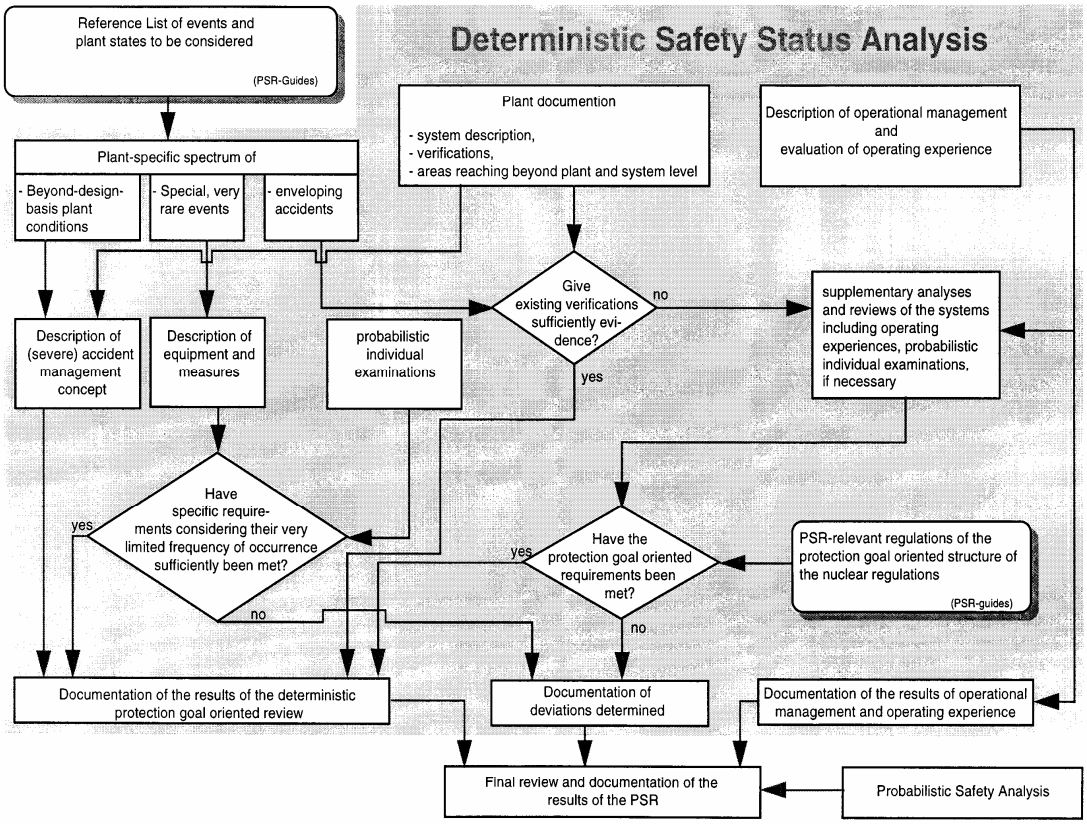

Fig. 2: Procedure of deterministic safety status analysis

4.2 Description of equipment and measures for special, very rare events as well as of (severe) accident management concept

For special, very rare events according to Appendix A, the equipment and measures of the plant which have to be taken to meet specific requirements are to be described. By incorporating probabilistic individual examinations, it should be shown that precautionary measures have been taken also for events with a very limited frequency of occurrence.

For beyond-design-basis plant conditions due to an assumed failure of demanded engineered safety features, on-site accident management measures are provided for all plants. These are generally structured in a protection goal oriented way and are based on using the safety margins of the plant, on the use of the operational systems and engineered safety features, and on additionally planned measures. All measures and actions are comprised in the accident management manual.

Measures of accident management as laid down in the accident management manual should be shown.

Description of the equipment and measures for special, very rare events should show that the plant can be transferred to a safe condition. Description of on-site severe accident management measures for beyond-design-basis plant conditions (cf. Appendix A) should show that they are suitable to avoid severe core damage or to reduce its consequences in such a way that the protection goals can be achieved.

Existing documents and verifications should be used for the description.

4.3 Description of operational management and evaluation of operating experience

The following parts of operational management should be described:
- plant organisation,
- plant operation,
- technical qualification,
- maintenance,
- radiation protection,
- experience feedback and
- accident management planning.

Main emphasis for assessing equipment and measures for keeping the protection goal oriented requirements on levels 1 and 2 is the evaluation of operating experience under the viewpoint of normal operation, anticipated operational occurrences and accidents.

The analysis of safety-related operating experiences should comprise the following areas:
- periodic testing and in-service inspections,
- load cases and fatigue analyses,
- reportable events.

In addition, the evaluation should consider such representative safety-related events (like reactor scram, turbine trip etc.) which are characteristic for the reliability of normal operation by the time sequence of their frequency of occurrence.

The evaluation of operating experiences serves for the review of proven operating experience of the safety-technical plant design, the review of reliability of safety relevant systems as well as the keeping of the safety objectives. The results should supplement and assure the statements made in the course of the deterministic protection goal oriented review of engineered safety features, especially for additional analyses and during the final review of the safety status of the plant.

The emphases for describing the areas of operational management as well as for evaluation of operating experiences are contained in Appendix D.

5 Results of the safety status analysis

The results of the safety status analysis should be composed in form of a report and should be presented to the supervisory authority as part of the documentation of the PSR.

It shall be possible to reconstruct and to examine the contents of the reports. The documents used have to be indicated.

The reports can be arranged as follows:

Report: Deterministic, protection goal oriented review
- accident analysis and protection goal oriented review of the systems,
- description of the severe accident management,
- list of documents used.

Report: Operational management and operating experience.

Following the deterministic review of the systems, a final assessment of the results considering the results of the PSA, the description of operational management and the evaluation of operating experience should be performed.

Final review of safety relevance of the deviations determined and the derivation of necessity and urgency of safety improvements should be performed in accordance with the specifications for evaluating the results of the PSR, as described in the „Basics of the PSR for Nuclear Power Plants“.

6 Appendices

Contents:

Appendix A

Reference list of the accidents to be considered, the special, very rare events and the beyond-design-basis plant conditions

Level 3, accidents,
events to be considered for transients

DWR-specific

- Primary-side, due to
  - withdrawal of most effective control element or most effective group during start-up,
- secondary-side, due to
  - loss of main heat sink caused by the failure to open of the main-steam turbine bypass system after turbine trip,
  - loss of main feedwater supply,
  - loss of off-site power supply,
  - leaks of main-steam lines up to $0.1A_D$ designed in a break preclusion quality, otherwise $2A_D$ (A_D: open cross-sectional area of the tube).

SWR-specific

- Reactivity accidents
  - limited failure of most effective control rod,
  - uncontrolled withdrawal of control rods during startup,
- loss of the main heat sink caused by spurious closure of the main-steam penetration valves,
- loss of main feedwater supply,
- loss of off-site power supply.

Level 3, accidents,
events to be considered for losses of coolant

PWR-specific

Leak cross-sections to be assumed for the reactor coolant boundary for plant-specific positions:
- leak cross-section < 120 cm²
  - overpressure protection systems stuck-open
  - break of connecting lines,
  - leaks at pipe branches, penetrations and seals,
  - leaks through cracks,
  - double-ended break of a steam generator tube in a steam generator,
- leak cross-section
  - about 0.1A (A: open cross-sectional area of a main coolant line designed in a break preclusion quality,
  - otherwise up to 2A.

SWR-specific

Leak cross-sections to be assumed for the coolant boundary for plant-specific positions:
- leak cross-section
  - about $0.1A_R$ (A_R : open cross-sectional area of tubes) when designed in a break preclusion quality, otherwise up to $2A_R$,
- leak cross-section smaller than 80 cm²
  - leaks through cracks in the area between the control rod drives of the reactor pressure vessel (RPV) bottom.

Level 3, accidents,
radiologically representative events

PWR-specific

- Losses of coolant with
  - leak cross-section A_{RL} (A_{RL}: open cross-sectional area of a measuring linein the annulus) caused by break of a measuring line in the annulus not isolated for 30 minutes,
  - leak cross-section $2A_{DE}$(A_{DE}: open cross-sectional area of a steam generator tube) and leak in the main-steam line behind the isolating valve considering the closing times of the isolating valve,
  - leak cross-section 0.1A designed in a break preclusion quality, otherwise up to 2A.
- fuel element handling accidents
  - damage of all outer-lying fuel rods of a fuel element,
- failure of auxiliary systems,
  - break of a line in the off-gas purification system,
  - failure of the waste water evaporator unit in the coolant treatment.

BWR-specific

- Losses of coolant with
  - Leak cross-section 2AAL (AAL: open cross-sectional area of a measuring line in the reactor building) caused by break of a measuring lance in the reactor building carrying reactor water not isolated for a period of 30 minutes,

- leak cross-section 0.1ANL (ANL: open cross-sectional area of a residual-heat removal line in themoval line in the reactor building during the shutdown phase taking into account closure times of the isolating valve,
- leak cross-section 0.1AR designed in a break preclusion quality, otherwise up to 2AR,

- leak cross-section smaller than 80 cm²
  - leaks through cracks in the area between the control rod drives of the reactor pressure vessel bottom,
- fuel element handling accidents
  - like PWR,
- failure of auxiliary systems
  - like PWR.

Level 3, accidents,
PWR and BWR-specific spreading impacts to be considered as possible iniating events for transients and small losses of coolant

Plant-internal impacts

- Flooding through leaks in pipes outside the coolant circuit of up to 0.1AR upon designed in a break preclusion quality, otherwise up to 2AR,
- other plant-internal flooding (e.g. through leaks in service water lines),
- plant-internal fires,
- fragments with high kinetic energy as a consequence of component failure (e.g. turbine missiles due to turbine blade failure).

Plant-external impacts

- Site-specific, external impacts caused by nature (earthquakes, lightning, flooding and weather conditions like wind, ice, snow).

Level 4,
PWR- and BWR-specific special, very rare events

- ATWS,
- Site-specific external civil impacts (certain emergencies).

Level 4,
beyond-design-basis plant conditions

PWR-specific

- Plant conditions owing to non-availability of engineered safety features challenged
  - loss of the entire steam generator injection system with a tendency towards a complete evaporation of the secondary sides,
  - loss of coolant with a small leak cross-section with the tendency to an increase of coolant pressure beyond the feed pressure of the high-pressure (HP) injection pumps,
  - double-ended break of a SG-tube in a steam generator and increase of main-steam pressure with the tendency towards actuating the main-steam safety valve,
  - loss of the entire three-phase current supply, if not battery-supplied for a period of up to 2 hours (station black-out),
  - global, long-term increase of pressure inside the containment vessel with the tendency towards an increase beyond design pressure.

BWR-specific

- Plant conditions owing to non-availability of engineered safety features challenged
  - Loss of coolant with subsequent overfeeding of one main-steam line and the possibility of water hammer outside the penetration isolation valve,
  - transients with the tendency of a decreasing of the RPV level to the lower edge of the core,
  - failure of the entire three-phase current supply, if not battery-supplied for a period of up to 2 hours (station black-out),
  - global, long-term increase of pressure in the containment vessel with the tendency towards an increase beyond design pressure.

Appendix B

Protection goal oriented structure of the nuclear regulations

The protection goal oriented structure of the nuclear regulations is to ensure in the performance of the safety status analysis a uniform application of the fundamental requirements of the nuclear regulations, as described in Sections 3.2 and 4.1.3 of the present guide „Safety Status Analysis“ in more detail, independent of individual technical solutions as well as including more recent, corroborate findings. It is to serve as a working basis or auxiliary means for the protection goal oriented review of the safety-related parts of the plant and for the evaluation of the results. Plant-specific particularities of a plant to be reviewed which are not considered in the protection goal oriented structure of the nuclear regulations have to be incorporated into the practical application.

During the elaboration of the PSR guides, a working group on the „protection goal concept“, consisting of technical experts of expert organisations, utilities and manufacturers, led by the BfS (Federal Office for Radiation Protection) and accompanied by representatives of the BMU (Federal Ministry for the Environment, Nature Conservation and Nuclear Safety), developed the protection goal oriented structure of the nuclear regulations and subsequently an outline of the fundamental requirements of the nuclear regulations.

This outline, in the version of December 1996 /1/, represents a separate part of the present guide „Safety Status Analysis“. [*)] It is planned to further develop this outline in the future.

The protection goal oriented structure of the nuclear regulations separates the fundamental criteria and requirements (levels II and III and Class A, cf. Fig. B-1) relating to the appropriate protection against ionising radiation from detailed implementation regulations and descriptions of measures (Level IV and Class B).

The national nuclear regulations, the basis of the protection goal oriented structure of the nuclear regulations on the sub-legal level comprises:

- safety criteria for nuclear power plants,
- RSK-guidances for PWR,
- accident guidances PWR,
- guidelines of the Federal States Committee for Nuclear Energy,
- safety standards of the Nuclear Standards Committee (KTA-Regeln),
- recommendations of the Reactor Safety Commission (RSK) and the Commission on Radiological Protection (SSK).

[*)] Note: Part A of the overview /1/ comprises a compilation of the superior requirements for the safety goals and is a result of the working group "*Schutzzielkonzep*t". Part B of the overview comprises a draft of the Federal Office for Radiation Protection (*Bundesamt für Strahlenschutz - BfS*) dealing with the fundamental requirements supporting functions common to all protection goals and was not discussed by the working group.

The subsequent Fig. B-1 shows the protection goal structure with 4 protection goals and 5 support functions common to all protection goals.

In addition, the requirements are also distinguished between the plant conditions normal operation and anticipated operational occurrences (levels 1/2), (design basis) accidents (level 3), special, very rare events (level 4a) and beyond-design-basis plant conditions (level 4b).

The subsequent extract from /1/ provides an outline of the 4 protection goals and the respective essential criteria as well as the requirements regarding support functions.

The 4 protection goals are:

Reactivity control

Reactivity control in all operational cases and accidents is ensured, if

- changes in reactivity and changes in the local power density are limited to permissible values by the inherent properties of the core in combination with the control, limitation and reactor protection actions,
- the reactor core can be shut down safely,
- fuel elements always remain subcritical during handling as well as in the storage facility for fresh fuel elements and in the spent fuel pool.

Cooling of fuel elements

Cooling of fuel elements is ensured if the heat generated in the fuel element can be removed during all operational cases and accidents. For this purpose,

- coolant and heat sinks have to be provided,
- transport of heat from the fuel element to the heat sink and
- heat removal from the spent fuel pool has to be ensured.

Confinement of radioactive material

The confinement of radioactive material is ensured if, even during an accident,

- the fuel remains sufficiently confined,
- leaks or cracks of the reactor coolant pressure boundary can be controlled and
- the integrity of the containment envelope is kept.

Limitation of radiation exposure

Limitation of radiation exposure is ensured, if:

- the activity inventory and flow in the plant are limited and controlled,
- the release of radioactive material is limited,
- building structures and technical equipment meet the requirements of radiation protection,
- radiation and activity in the plant and the environment are monitored and administrative regulations take radiation protection sufficiently into account.

The 5 support functions (see /1/) are:

- reliability,
- overall design (protection against external and internal impacts),
- administration,
- instrumentation and control,
- energy and support-media supply.

References

/1/ Arbeitsgruppe Schutzzielkonzept: Schutzzielorientierte Gliederung des kerntechnischen Regelwerks - Übersicht über die übergeordneten Anforderungen - Dezember 1996
BfS-KT-17/97

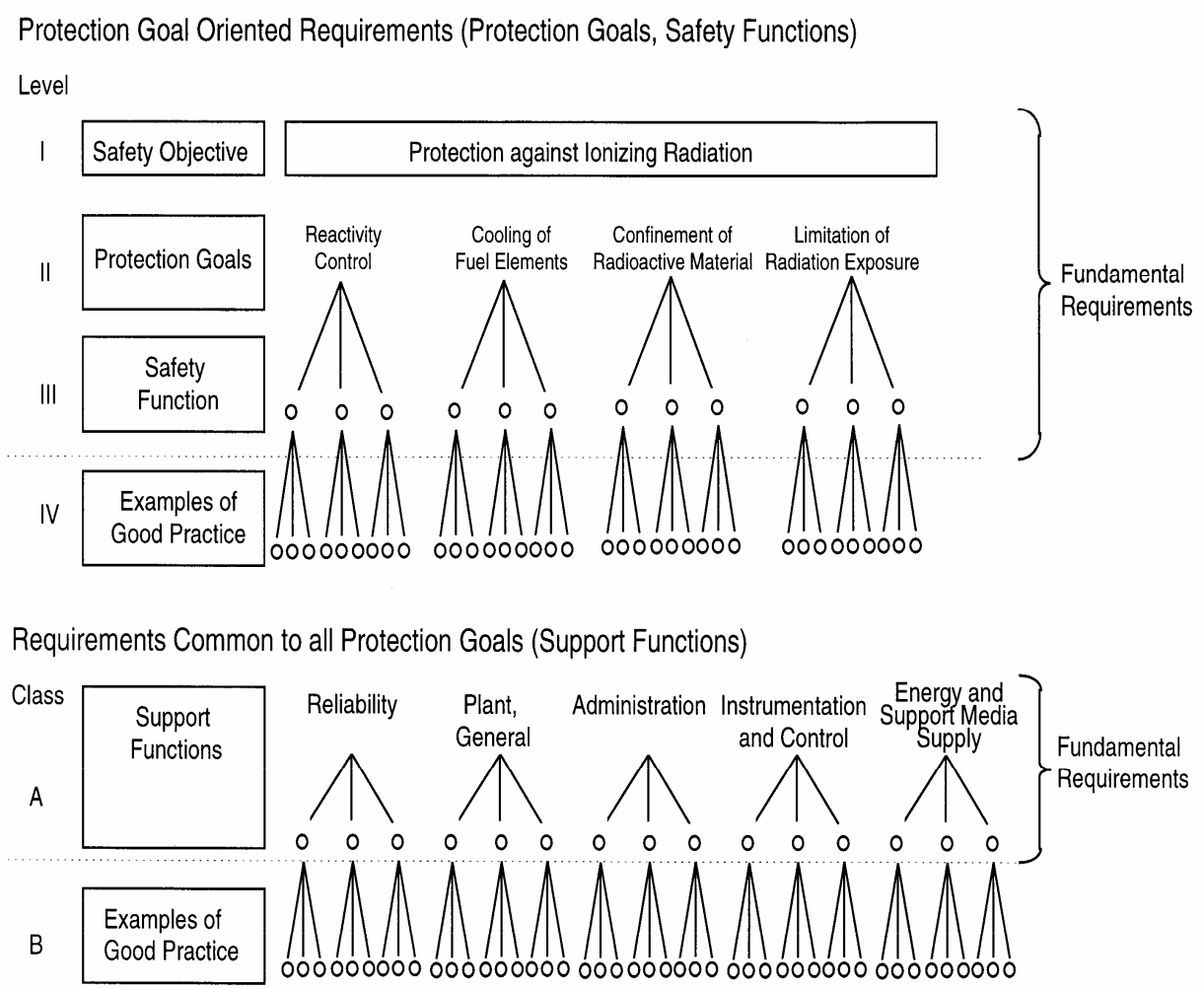

Fig. B-1: Scheme of the protection goal oriented structure of the nuclear regulations

Appendix C

Outline for the structure of system descriptions

1 Functions of the systems
1.1 Safety functions
1.2 Operational functions

2 System design and spatial arrangement
2.1 System connection/system flow diagram
2.2 Supply systems
2.3 Important components
2.4 Spatial arrangement

3 Operating modes of the system
3.1 Original position/normal operation
3.2 Accidents
3.3 Actuation criteria and protective actions
3.4 Interaction with other systems
3.5 Beyond-design-basis accidents

4 Design
4.1 Operational design
4.2 Accident-related design
4.3 Stress-related design
4.4 System protection and important interlocks
4.5 Instrumentation, control, monitoring

5 Functional testing and quality status

6 Compilation of data

7 References

Appendix D

Topics related to the description of operational management and the analysis of operating experience

Description of operational management

1 Operational organisation
- description of the organisational structure,
- staff,
- responsibilities,
- quality assurance concept.

2 Plant operation
- Operational diagrams illustrating the essential events,
- operating availability, energy availability factor,
- unplanned shutdowns,
- reactor scrams from power operation,
- safety related reportable events classified as INES-level 1.

3 Technical qualification of personnel
- measures for maintaining technical qualification,
- programmes, organisation and results of training measures,
- qualification of new employees.

4 Maintenance
- brief description of maintenance strategy,
- preventive maintenance during power operation,
- non-availability of safety systems due to maintenance,
- essential results of maintenance measures.

5 Radiation protection
- organization, if not dealt with under no. 1,
- dose rate level in the plant,
- activity concentration in systems and room airborne activity,
- radiation exposure of staff,
- activity-related radiation exposure of the staff,
- documentation, strategy and equipment,
- emission of radioactive substances via exhaust air, waste water and radioactive waste.

6 Experience feedback
- organisation,
- consequences from experiences in domestic and foreign plants,
- list of measures taken.

7 Accident management planning
- brief description of the strategy,
- emergency response staff,
- alarm plan, accident management manual,
- exercises.

Analysis of Operating experience

1 Results of periodic testing and in-service inspections, especially
- Pressure test of the pressure boundary,
- Non-destructive inspection of the pressure boundary,
- Steam generator tube testing,
- Reactor containment leak rate testing,
- Functional testing of important safety systems.

2 Load cases and fatigue analyses,
- operational load cases and load cases due to disturbances,
- fatigue analysis,
- service life monitoring of components.

3 Evaluation of reportable events

Guide Probabilistic Safety Analysis

Contents

1 Introduction

For nuclear power plants with light water reactors in operation in the Federal Republic of Germany, a safety review (Periodic Safety Review-PSR) is to be carried out at intervals of ten years. The Probabilistic Safety Analysis is part of the PSR.

Nowadays, Probabilistic Safety Analyses (PSA) belong to the state of the art in science and technology in safety assessment of nuclear power plants. With the help of these analyses statements on the balance*) of the safety concept can be made and potentially existing vulnerabilities can be determined. PSAs are employed in addition to the technical safety assessment having deterministic bases.

The present guide describes the objective of the PSA and lays down the procedure as well as the scope of the PSA. The guide takes the experiences acquired in the performance and assessment, as well as in expert examinations of probabilistic safety analyses in the Federal Republic of Germany as an orientation.

2 Objective and scope of the probabilistic safety analysis

Within the framework of the PSR, the PSA serves for the verification of the balance of the safety concept with respect to keeping the protection goals of core cooling and confinement of radioactive material. Apart from other aspects, PSA can also be used for evaluating the safety level.

The objectives of the probabilistic safety analysis are:
- to determine and quantify event sequences which

*) Explanation of the term see Appendix A

can lead to a hazard for fuel element cooling. The active functions of the containment envelope[*)] have to be considered in the probabilistic safety analysis,
- to determine quantitative values of frequencies of occurrence of these events,
- to evaluate the balance of the safety concept and to determine vulnerabilities.

This target is achieved by means of a PSA Level 1+ which is the subject of this guide.

A level 1+ analysis is obtained by extending the system analyses of level 1 by including the active functions of the containment envelope.

Determined are those event sequences that lead to hazard states, which consequently can lead to core damage unless further measures are taken and where an impairment of confinement of radioactive material cannot be excluded in the further course.

To transfer hazard states into safe plant conditions or to mitigate damage, accident management measures have been introduced in the nuclear power plants. Such measures can additionally be evaluated probabilistically to determine the frequency of damage states[*)].

Event sequence and fault tree analyses together with importance, sensitivity and uncertainty analyses have to be carried out with respect to the operating conditions for a wide spectrum of initiating events[*)]. Success criteria have to be determined depending on the event sequences. Plant technology as well as operating modes of the systems are to be modelled adequately. Dependencies between system functions, common cause failures as well as human actions have to be considered. Plant-specific reliability parameters[*)] should be used as far as possible. The quantitative analyses have to take the targets of the PSA into account. The event sequence paths shall be categorised with respect to the resulting plant conditions.

Details referring to the above-mentioned points are laid down in the subsequent sections of this guide as well as in /1/ and /2/.

3 Probabilistic safety analysis

3.1 General

The PSA comprises the substantial work steps shown in the flow chart (Fig. 1) which is briefly described below. Details are shown in /1/ and /2/.

When performing a PSA, models and partial results from the respective analyses of comparative plants can generally be used. It shall be ensured that the technical conditions and operating modes of the plants are in accordance as far as they have to be determined in the course of the analyses

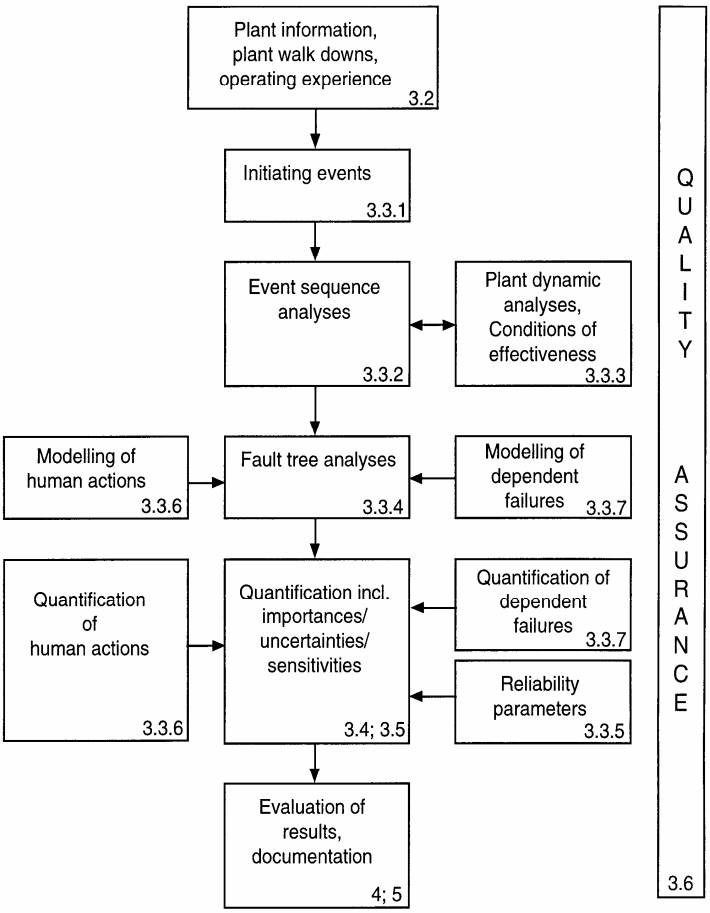

Fig. 1: Flow chart of the Probabilistic Safety Analysis (PSA) within the framework of the Periodic Safety Review (including references to the respective sections in the present guide)

[*)] Explanation of the term see Appendix A

3.2 Plant-specific initial information

To perform a PSA, detailed information on the structure, functions and efficiencies of components and systems to be considered are necessary including operating measures, operating modes, maintenance measures and periodic testing and in-service inspections. In general, this information can be derived from the existing documentation describing the plant. This documentation contains descriptions of the systems, circuit diagrams, operating and inspection manuals and, possibly, emergency manuals as well as analyses of accidents on which the design of the engineered safety features of the plant is based. The PSA must generally be based on the plant status at a fixed point in time. Backfitting measures and accident management measures which have not yet been implemented can be incorporated into the PSA if they have been licensed or if an application for them is prepared in a verifyable way.

Important and supplementary information is to be derived from plant walk downs, operating experiences as well as from expert talks with the operating personnel (e.g. on specific operational processes during human actions).

3.3 Methods of analysis

The methods to be applied for the PSA in the course of the PSR will briefly be described below. Details of the methodological procedures of the probabilistic analysis and the collection of data have been illustrated in /1/ and /2/.

3.3.1 Initiating events

Initiating events resulting from other PSAs and investigations available so far are comprised in Appendices B1 and B2. These are reference spectra of initiating events to be considered which have to be examined, verified and, if necessary, to be modified (e.g. leak size). Furthermore, additional initiating events which are possibly also to be analysed are listed in /1/ which take the results of incident analyses as well as plant-specific investigations into account.

The spectrum of initiating events to be considered shall be justified plant-specifically with respect to completeness, especially with regard to a complete acquisition of all relevant events. Relevant intitiating events of /1/ which may to be considered additionally shall be analysed in the course of updating the PSA. It appears expedient that the required agreement between the licensee and the authorities should be reached at the beginning of the PSA.

For the initiating events under consideration, the operational conditions of full power operation shall be considered first. Standstill, startup and shutdown conditions shall be considered for respective initiating events if corresponding methods have been developed and if there is information from German operating experience referring to essential contributions of these plant conditions with respect to the overall risk of the plant.

3.3.2 Event sequence analyses

Depending on the initiating event and the respective operational condition of the plant, those functions of operational and safety systems*) as well as the manual actions shall be determined which are designed and required for controlling the event sequence. The activation criteria for the systems controlling accidents represent the main basis of this determination. In addition, manual actions of the operating personnel can be taken into account. The conditions of efficiency of the individual systems shall be determined depending on the event sequence. Plant conditions which are not controlled by the safety systems shall be assigned to the hazard states and shall be characterisedaccordingly. The hazard states shall be subdivided into different categories /1/, taking into account the time sequences of the individual event sequence paths and their possible consequences.

In addition, probabilistic estimations on existing accident management measures in the beyond-design-basis area can be taken into account. These shall be listed separately event sequence diagrams.

3.3.3 Analyses relating to conditions of efficiency

The conditions of efficiency describe the minimum requirements to be met by the individual functions of the systems as well as the respective mission times of the systems in case of demand. The determination of the conditions of efficiency should preferably be carried out on the basis of computations with realistic boundary conditions so that the existing safety margins of the plant can be considered in the analysis and thus enables an assessment of the balance of the safety concept as close to reality as possible is. To reduce investigation efforts, conservative computations of the licensing procedure can be used under the precondition that these analyses can be applied to the event sequence under consideration with regard to initial and boundary conditions.

3.3.4 Fault tree analyses

System parameters (non-availabilities or failure probabilities) of the requested system functions during the respective mission times are required for a quantitative analysis of the event sequence diagrams. These parameters are determined with the help of fault tree analyses /1/. Dependencies between system functions shall be considered here.

The elaboration of fault trees, where the failure of the system can be attributed to the failures of partial systems and their failures to the failure of components, in individual cases can be supported by the use of inductive analysis procedures.

Details on a fault tree analysis are shown in /1/.

3.3.5 Reliability parameters

Plant-specific reliability parameters should generally be used in the analysis to acquire the condition of the plant as realistically as possible. If generic data are used, a plant-specific analysis shall be carried out for those components whose independent failures determined with this set of data provide essential contributions to the total frequency of the hazard states. The necessary information for a plant-specific collection of reliability parameters shall be determined from the operational records of the plant. The procedure is shown in /2/.

The data basis, in connection with the probabilities for incorrect human actions and common cause failures (CCF), serves for the quantification of fault trees and event sequence diagrams.

3.3.6 Human actions

The analysis of human actions comprises the identification, modelling and probabilistic assessment of incorrect actions by the operating personnel having effects on event sequences. The functions asked for in the course of an event sequence can depend on human actions in different ways.

Details on the analysis of human actions in a PSA are shown in /1/.

3.3.7 Dependent failures

Dependent failures shall be considered in the fault tree analysis. Subsequent failures and functional dependencies (e.g. joint dependency on an auxiliary system) are modelled explicitly, the remaining dependent failures (CCF) can be incorporated into the fault trees via parametric models. Details are shown in /1/.

3.4 Computation codes

The quantitative analysis of the event sequence diagrams and fault trees shall be performed with a generally acknowledged computation programme, which allows, among other things, to take into account the influence of the variations of the reliability parameters on the final result and to determine the importances and sensitivities. The requirements to be met by such computation programmes are laid down in /1/.

3.5 Performance of the analysis and determination of the results

The event sequence diagrams are analysed quantitatively considering the objectives of the probabilistic safety analysis defined in Section 2. Frequencies of occurrence of event sequences leading to hazard or damage states and showing the relevant influences on these probabilities shall be determined as the result of the analysis. The hazard and, if necessary, damage states are to be shown separately. Furthermore, the non-availabilities of system functions (including the active systems of thecontainment envelope) shall be determined.

3.6 Quality assurance

During the performance and the evaluation of the PSA, quality assurance for the individual work steps of the PSA shall be ensured, also with reference to the plant personnel. Measures and results of quality assurance are to be illustrated (those results of quality assurance which were implemented immediately as a correction in the PSA do not have to be shown specifically).

4 Evaluation of the results

The results of the PSA shall serve as a supplement to the deterministic review of the safety status of the plant for evaluating the balance of the safety concept and for determining the necessity and the urgency of safety improvements required.

The balance of the safety concept should be evaluated from different viewpoints (e.g. frequency of the initiating events, frequency of event sequence paths) and possible vulnerabilities should be identified.

The evaluation shall be carried out with the help of the qualitative as well as the quantitative results of the analyses. Different categories of hazard states owing to time sequence and possible consequences shall be considered during the evaluation.

Uncertainties of the quantitative results due to the variations of the reliability parameters shall also be considered in the assessment. In addition, importance and possibly also sensitivity computations shall be carried out to show relevant influences of uncertainties during the determination of reliability parameters of components or during the determination of probabilities of common cause failures and incorrect human actions on the result.

5 Report on probabilistic safety analysis

Documentation of preparation and performance of analyses, measures for quality assurance and results of probabilitistic safety analysis shall be designed in such a way that the analysis, the results and the evaluation are reconstructable, that practical applications are feasible and that it is ensured that the PSA can be updated (Living PSA).

The topics mentioned below shall be dealt with:
- documents used;
- initiating events and event sequences analysed as well as justification of the spectrum of events analysed;
- analyses of efficiency;
- event sequence and fault tree analyses;
- documentation of the computer analysis;
- reliability parameters used;
- component models used for independent and common cause failures;
- assessment of human actions;
- quality assurance as well as
- results and evaluation of results

6 References

/1/ Facharbeitskreis Probabilistische Sicherheitsanalyse für Kernkraftwerke: Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke - Dezember 1996 - BfS.KT-16/97

/2/ Facharbeitskreis Probabilistische Sicherheitsanalyse für Kernkraftwerke: Daten zur Quantifizierung von Ereignisablaufdiagrammen und Fehlerbäumen - April 1997 - BfS-KT-18/97

Appendix A

Explanation of terms used

Balance of the safety concept

The safety concept shall be considered wall balanced if the individual contributions (such as frequencies of hazard states for initiating events or for event sequence paths) do not dominate the respective result.

Containment envelope

The containment envelope is the system consisting of containment vessel and the surrounding building as well as auxiliary systems to retain and filter possible leakages from the containment vessel.

Initiating event

Disturbances and damages to components and parts of the plant initiating an actuation of the safety systems are called "initiating events".

Plant-specific reliability parameters

Parameters which are employed to determine the reliability of components or systems (failure rates, failure probabilities) are called reliability parameters. Plant-specific reliability parameters are parameters based on data and information from the plant which have to be recorded in an appropriate way. To estimate the plant-specific reliability parameters, generic advance information is generally to be taken into account in an adequate way (Bayes' Methodology).

Hazard state

Plant condition where the protection goals, such as the confinement of radioactivematerial, cooling of fuel elements, are no longer under the control of the systems designed for this purpose. Without further measures, a damage state can arise. It is possible that a hazard state can be transferred into a safe plant condition with the help of severe accident management measures and that a damage state can thus be prevented.

Plant condition from which a loss of barriers can develop so that the confinement of radioactive material is no longer guaranteed. This can be: core damage, severe core damage, core meltdown or larger damage to fuel elements outside the reactor core (e.g. in the spent fuel pool). Severe accident management measures can be provided to keep radiological damage inside and outside the plant as low as possible.

Safety system

The safety system is the entirety of all systems of a reactor plant having the task of protecting the plant against unpermissible stress and, if accidents should occur, of keeping their effects on the operating personnel, the plant and its environment within the preset limits.

Operational system

The operational system comprises all the systems, circuits and auxiliary systems which are only required for the normal operation including anticipated operational occurrences. These have to be designed in such a way that accidents as a consequence of abnormal operational conditions are prevented with sufficient reliability.

Reference spectrum of initiating events for a pressurised water reactor

	Leaks in a main coolant line	leak cross-section (cm^2)		
1	large and medium-sized leak		>	200
2	small leak 1	80	-	200
3	small leak 2	50	-	80
4	small leak 3	25	-	50
5	small leak 4	25	-	50
6	small leak 5	2	-	12
	Pressuriser leaks	leak cross-section (cm^2)		
	small leak at the pressuriser caused by transients:			
7	due to loss of main feedwater supply	20		
8	due to loss of main heat sink	20		
9	due to other transients	20		
10	small pressuriser leak due to inadvertent opening of a safety valve	40		
	Leak in a connecting line in the annulus	leak cross-section (cm^2)		
11	leak	2	-	500
	Steam generator tube leak	leak cross-section (cm^2)		
12	small leak 1	6	-	12
13	small leak 2	1	-	6
	Operational transients			
14	loss of off-site power			
15	loss of main feedwater supply without loss of main heat sink (long-term)			
16	loss of main feedwater supply and loss of main heat sink			
17	loss of main heat sink without failure of main feedwater supply			
18	overfeeding of steam generator			
	Transients caused by leaks in the main-steam lines			
	large leak:			
19	inside the containment vessel			
22	outside the containment vessel			
	medium-sized leak:			
21	inside the containment vessel			
22	outside the containment vessel			
	Transients caused by leaks in the feedwater lines			
	large leak:			
23	inside the containment vessel			
24	outside the containment vessel			
	medium-sized leak:			
25	inside the containment vessel			
26	outside the containment vessel			
	Anticipated transients without scram (ATWS)			
27	ATWS due to loss of main feedwater supply			
28	ATWS due to loss of off-site power			
29	ATWS due to loss of main heat sink and main feedwater supply			
30	ATWS due to other transients			
	Plant-interfacing impacts			
31	flooding of safety relevant parts of the building due to plant-internal causes			
32	fire			

Appendix B2

References spectrum of initiating events for a boiling water reactor

	Leak accidents inside the containment vessel
1	leaks in main-steam lines having different sizes
2	feedwater line leaks having different sizes
3	leak in the RPV bottom
4	leak in the reactor water purification system
	Leak accidents outside the containment vessel
5	leaks in the main-steam lines having different sizes
6	leaks in the auxiliary steam lines having different sizes
7	leaks in the feedwater lines having different sizes
8	leaks in the reactor water purification system
	Other leaks
9	leaks having different sizes in the pressure suppression pool, e.g. outside the containment vessel (break of a connecting pipe)
10	leak in a service water line
11	break of a line carrying river water into the turbine hall
12	leak in the residual-heat removal system during residual-heat removal operation
	Transients
13	loss of the main heat sink
14	loss of the feedwater supply system
15	loss of off-site power
16	anticipated transients without scram (ATWS)
17	inadvertent opening or remaining open of a S&R valve
18	inadvertent opening of turbine and by-pass control valves
19	overfeeding transient
	Plant-interfacing impacts
20	flooding of safety relevant parts of the buildings due to plant-internal cause
21	fire