Safety Criteria for Nuclear Power Plants

REVISION D

JUNE 2009

Note:

This is a translation of the document entitled: "Sicherheitskriterien für Kernkraftwerke".

In case of discrepancies between the English translation and the German original, the original shall prevail.

A

MODULE 1
"Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria"

Contents

0 Fundamental principles

The fundamental safety objective is the protection of man and the environment against the harmful effects of ionising radiation. This objective applies to all activities from planning through the construction and operation to the dismantling of a nuclear power plant.

The licensee is responsible to assure plant safety. He gives preference to meeting the safety objective over other plant operational objectives.

The basis of the safe operation of a nuclear power plant is the safety-oriented interaction of human, technical and organisational factors (man-technology-organisation). The interconnection of these factors with the objective of taking actions in a safety-oriented manner is also the basis for a highly developed safety culture. To maintain this safety culture and to enhance it continuously is the task of the licensee.

1 Organisational criteria

1 (1) Licensees with a highly developed safety culture have a safety management system in place summarising the objectives and activities of all areas of the company that are aimed at ensuring safe plant operation. The company of the licensee is organised as a self-learning system.

The safety management system comprises the entirety of all activities and processes for the proper planning, organisation, management and control of personnel and working activities. The objectives of safety management are

- to ensure safety
- to enhance safety continuously, and
- to promote safety culture.

Safety management promotes the self-critical behaviour and the critical and questioning attitude of all staff as well as the trustful co-operation in all areas within the company of the licensee.

The realisation of the objectives of safety management requires the guarantee of a high degree of quality of the safety-relevant infrastructure, activities and processes, including the trustworthiness, the technical qualification and the social competence of the personnel.

1 (2) The realisation of the safety management requires a management system which integrates all regulations and organisational aids to carry out safety-relevant activities and processes.

1 (3) The boundaries and the interfaces as well as the interactions and interdependencies within the management system of the company of the licensee are specified and regulated in such a way that the safety objective is not impaired by other business objectives. The relation with external organisations is regulated correspondingly.

The management system is suitable for providing indications of potential safety impairments at an early stage.

The management system is designed as a closed "plan-do-check-act (PDCA) management cycle". This cycle is also applied to all activities and processes of the management system.

1 (4) The management system meets the following requirements:

a) The safety policy demonstrates the licensee's commitment to a highly developed safety culture. It underlines the priority of safety over all other business objectives. To implement the safety policy, clear, measurable and consistent safety objectives are developed and measures are derived to achieve these objectives.
b) The required material, human and financial resources to meet the safety objectives are provided. These resources comprise:

- the infrastructure, including the plant to be safely operated,
- a sufficient number of suitable and qualified personnel with the required trustworthiness, qualification (technical qualification and practical experience) and the social competencies;

the furtherance of technical qualification is ensured by training, instruction and further qualification,
- appropriate financial means to support the safety of the nuclear power plant during its entire operating lifetime,
- an ergonomically adequate working environment and working conditions, and
- well-regulated co-operation with external organisations.

c) Functions and authorisations (authorisations to take decisions and to issue instructions) and thus the responsibilities are clearly allocated within the company of the licensee as far down as to the execution level, are agreed by those concerned, and are announced and implemented. A gapless delegation of responsibilities is ensured.
d) All safety-relevant activities and processes are planned, performed, monitored and - if necessary - improved at a high level of quality. The interfaces between the activities or processes are defined.
e) It is ensured that safety-related activities are only performed by personnel that is suitable to do so.

1 (5) The management system is regularly reviewed at appropriate time intervals and whenever any relevant new insights are available; it is enhanced if necessary.

1 (6) The planning, performance, review and improvement of the management system is documented systematically and comprehensibly.

2 Technical safety concept

2 (1) For the safe confinement of the radioactive materials present in the nuclear power plant, a defence-in-depth safety concept is realised that combines meeting the radiological safety objectives (see Section 2.4) with the multiple confinement of the radioactive materials by barriers, supported by retention functions (see Section 2.2) and the protection of the barriers and the retention functions by measures and installations on several consecutive levels of defence (see Section 2.1).

2.1 Defence–in-depth concept

2.1 (1) Confinement of the radioactive materials present in the nuclear power plant is ensured.

In order to achieve this objective, a safety concept is implemented in which measures and installations are allocated to different levels of defence which are characterised by the following plant states:
- Level of defence 1: normal operation (specified normal operation)
- Level of defence 2: abnormal operation (specified normal operation)
- Level of defence 3: accidents
- Level of defence 4a: very rare events
- Level of defence 4b: events with multiple failure of safety installations
- Level of defence 4c: accidents involving severe core damage (here, the goal is to maintain the confinement of the radioactive materials as far as possible).

2.1 (2) Furthermore, measures for supporting disaster control are planned for accidents involving severe core damage in which considerable releases of radioactive materials to the environment cannot be prevented or limited by accident management measures, level of defence 5.

N o t e: The relevant requirements are included in the disaster control regulations of the *Länder*.

2.1 (3a) The safety concept is designed to be preventive. Measures and installations are provided which

on level of defence 1

a) prevent the onset of anticipated operational occurrences and accidents,
b) prevent events with multiple failure of safety installations,

on level of defence 2

a) control any on setting anticipated operational occurrences,
b) prevent the onset of accidents,
c) prevent events involving the multiple failure of safety installations,
on level of defence 3
a) control accidents,
b) prevent the onset of events involving the multiple failure of safety installations,
on level of defence 4a
a) control the effects of very rare events,
on level of defence 4b
– in the case of events involving the multiple failure of safety installations prevent severe core damage (preventive accident management measures).

2.1 (3b) On level of defence 4c, measures are provided which in the case of an accident involving severe core damage limit the release of radioactive materials into the environment as far as possible (mitigating accident management measures).

2.1 (4) The defence-in-depth concept is implemented at the plant for all plant operating phases, with consideration of the respective special features of the different operating phases.

2.1 (5) On levels of defence 2 and 3, measures as well as installations are provided that are arranged in such a way that upon the failure of measures and installations on levels of defence 1 and 2, the measures and installations on the subsequent level re-establish the required safety-related condition independent of measures and installations of other levels of defence.

Measures and installations that have to be effective on all or on several of these levels of defence are designed such that they can withstand the impacts associated with these levels in accordance with the criteria that apply to these levels.

2.1 (6) It is ensured that a single technical failure or erroneous human action on one of the levels of defence 1 to 3 will not jeopardise the effectiveness of the measures and installations on the next level.

2.1 (7) If using measures and installations provided on the level of defence 2 or 3 to show that the criteria of previous levels of defence are met it is demonstrated that
– other technical solutions are not reasonable, and
– negative effects on the reliability and effectiveness of the measures and installations used for the control of events are excluded.

2.1 (8) On level of defence 4, appropriate measures and installations of the levels of defence 1 to 3 are also used apart from the measures and installations specially provided for this level.

2.1 (9) The measures and installations specially provided for accident management on levels of defence 4b and 4c are not used on the other levels of defence according to the design.

2.1 (10) Quality and reliability of the nuclear power plant's installations correspond to their respective safety significance.

All safety-relevant installations are classified according to their safety significance. The criteria for quality and reliability applicable in the specified classes are defined and include, in particular, specifications on requirements with regard to design, manufacturing environmental and effectiveness conditions, emergency power supply and long-term maintenance of quality.
Of highest safety significance and accordingly classified are:
a) installations whose failure leads to event sequences that cannot be controlled, and
b) installations that are necessary for effective and reliable accident control, including the auxiliary and supply systems required for it.
Of graded safety significance and accordingly classified are:

a) installations that are necessary for effective and reliable accident prevention, including the auxiliary and supply systems required for it,
b) installations for compliance with and monitoring of defined radiological limits, particularly by maintaining the required effectiveness of barriers and retention functions,
c) installations performing safety-related functions that do not belong to the previous classes.

2.1 (11) The measures and installations on all four levels of defence are principally available for the different plant operating phases according to the criteria specified for them. Any unavailabilities are limited depending on their safety-related consequences, the associated conditions that have to be fulfilled are specified.

2.1 (12) The measures and installations of levels of defence 1 to 4a meet most stringent requirements with regard to the quality and reliability of planning, implementation and performance of the measures and the design, manufacturing, construction and operation of the installations

For the measures and installations specifically provided for levels of defence 4b and 4c, graded requirements are applicable.

2.1 (13) To support disaster control, measures are provided inside and outside the plant to determine the consequences of accidents with potential or actual releases of radioactive materials and to mitigate as far as possible their effects on man and the environment (level of defence 5).

The measures to be taken in case of disaster are regularly trained in exercises.

The licensee participates in the official disaster control planning and provides his own prevention and protection measures, which are included in the plant operating procedures.

2.2 Concept of the multi-level confinement of the radioactive inventory (barrier concept)

2.2 (1) The confinement of the radioactive materials present inside the nuclear power plant is ensured by sequential barriers and retention functions. The barriers and retention functions are designed in such a way and maintained in such a condition over the entire plant operating lifetime that, in combination with the measures and installations of the respective levels of defence, the respective safety-related acceptance targets and acceptance criteria as well as the radiological safety objectives according to Section 2.4 are met on the different levels of defence for all events or plant states and the associated mechanical, thermal, chemical and radiation-induced impacts.

2.2 (2) If barriers are ineffective due to planned operational procedures, other measures and installations are available to achieve the radiological safety objectives (see subsection 2.4 (1)) which ensure an effective and reliable retention function according to the respective conditions.

2.2 (3) On levels of defence 1 and 2, the following barriers are effective - apart from the retention functions - to achieve the radiological safety objectives:
a) for the confinement of the radioactive materials in the reactor core:
1. the fuel rod cladding, except for admissible, operationally induced cladding damage,
2. the reactor coolant pressure boundary, unless the reactor coolant system is not opened according to scheduled, and
3. the containment, unless it is not opened according to schedule. The opening of the containment according to schedule is not performed before reaching specified pressure and temperature conditions in the reactor coolant system.

b) for the confinement of the radioactive materials in irradiated fuel elements that are handled or stored within the plant
1. during operating phases A to F, the fuel rod cladding, except for admissible, operationally induced cladding damage, as well as
2. the containment, unless it is not opened as schedule. If irradiated fuel elements are handled or stored outside the containment or if the containment is opened according to schedule, the non-existence of a containment is compensated by retention function.

The safe controlled confinement of the radioactive materials elsewhere in the plant is ensured in all operating phases by retention functions.

2.2 (4) On level of defence 3, the following barriers are effective - apart from the retention functions - to achieve the radiological safety objectives:
a) for the confinement of the radioactive materials in the reactor core
1. the fuel rod cladding, unless their failure is postulated as initiating event and not in event of a large-break loss-of-coolant accident,
2. the reactor coolant pressure boundary, unless the reactor coolant system is not opened according to scheduled and its failure is not postulated as initiating event,
3. the containment, unless it is not opened according to schedule. If the containment is opened according to schedule, it is ensured that the barrier function of the containment is restored in due time to the necessary extent in the case of events with releases of radioactive materials within the containment.
b) for the handling and storage of fuel elements
1. the fuel rod cladding (except for cladding damage specifically postulated case by case for each event), as well as
2. the containment, unless it is not opened according to schedule. If the containment is opened according to schedule, it is ensured that the barrier function of the containment is restored in due time to the necessary extent in the case of events with releases of radioactive materials within the containment.

   If irradiated fuel elements are handled or stored outside the containment or if the containment is opened according to schedule, the non-existence of a containment is compensated by retention functions.

The achievement of the radiological safety objectives with regard to radioactive materials elsewhere in the plant is ensured in all operating phases by retention functions.

2.2 (5) On level of defence 4a, the following barriers are effective with regard to the reactor core:
1. the fuel rod cladding to the extent necessary for meeting the acceptance targets applicable here,
2. the reactor coolant pressure boundary, unless the reactor coolant system is not opened according to schedule,
3. the containment, except for external mechanical impacts and unless it is not opened according to schedule.

With regard to the radioactive materials in irradiated stored fuel elements, the barrier of the fuel rod cladding is effective.

2.2 (6) On level of defence 4b, the aim of the planned accident management measures - apart from maintaining the function of retaining the activity inventory of the reactor core – is to
- maintain the integrity of the fuel rod cladding in the case of event sequences involving containment bypass, and otherwise to
- maintain the retention function of the containment system.

For the confinement of the radioactive materials in the irradiated stored fuel elements, the aim on level of defence 4b is to maintain the integrity of at least one barrier.

On level of defence 4c, the aim of the planned accident management measures is to maintain containment integrity for as long as possible.

2.3 Concept of the fundamental safety functions (protection goals)

2.3 (1) By the measures and installations provided according to subsection 2.1 (3a), the following fundamental safety functions (protection goals) are achieved for the criteria applicable on the respective levels of defence:
a) reactivity control,
b) fuel cooling, and
c) confinement of the radioactive materials.

2.3 (2) On levels of defence 1 to 4a, the following criteria are met:

for reactivity control:
- reactivity changes are restricted to values that have been demonstrated as being admissible,
- the reactor core can be shut down safely and can be kept subcritical in the long term ,
- upon the handling of fuel elements and in the storage for fresh fuel elements as well as in the fuel element storage pool, subcriticality is ensured;

for fuel cooling:
- coolant and heat sinks are always sufficiently available,
- heat transfer from fuel to heat sink is ensured,
- heat removal from the fuel element storage pool is ensured;

for the confinement of the radioactive materials:
- the mechanical, thermal, chemical and radiation-induced impacts resulting on the different levels of defence are limited such that the radiological safety objectives according to Section 2.4 are achieved and that fuel cooling is ensured.

2.3 (3) On level of defence 4b, the aim is to reach long-term compliance with the protection goals by accident management measures

2.3 (4) On level of defence 4c, the aim is to maintain by accident management measures the integrity of the containment for as long as possible, to retain the radioactive materials to the furthest possible extent and to reach a long-term controllable condition.

2.4 Radiological safety objectives

2.4 (1) On levels of defence 1 and 2
- radiation exposure of the personnel is kept as low as achievable for all activities, even below the limits of the Radiation Protection Ordinance, taking into account all circumstances of individual cases,
- any discharge of radioactive materials with air or water is controlled via the specially provided release paths; the releases are monitored as well as documented and specified according to their kind and activity; and
- any radiation exposure or contamination of man and the environment by direct radiation from the plant as well as by the discharge of radioactive materials is kept as low as achievable, even below the limits of the Radiation Protection Ordinance, taking into account all circumstances of individual cases.

On level of defence 3
- the maximum radiation exposure limits for the personnel in connection with the planning of activities for the control of events, the mitigation of their effects or the elimination of their consequences do not exceed the relevant limits of the Radiation Protection Ordinance
- the maximum design limits for the plant for protecting the population against any release induced radiation exposure do not exceed the relevant accident planning levels of the Radiation Protection Ordinance,
- any release will only happen via specially provided release paths; the release is monitored and is documented and specified according to its kind and activity; and
- the on-site and off-site radiological consequences are kept as low as achievable, taking into account all circumstances of individual cases.

On level of defence 4

- the relevant limits of the Radiation Protection Ordinance are applied to the expected radiation exposure of the personnel for the planning of activities for the control of events on level of defence 4a and for the planning of activities within the framework of accident management measures,
- the monitoring of releases of radioactive materials from the plant according to their kind and activity is ensured, and
- on-site and off-site radiological consequences are kept as low as achievable, taking into account all circumstances of individual cases.

2.4 (2) All safety-relevant installations of a nuclear power plant are designed in such a way, maintained in such a condition and protected in such a manner against impacts that they fulfil the safety-related functions for meeting the criteria according to subsection 2.4 (1).

All installations of a nuclear power plant that contain or may contain radioactive materials are conditioned, arranged and shielded in such a way that the relevant criteria according to subsection 2.4 (1) are met with regard to the radiation exposure of individuals for all necessary activities on levels of defence 1 and 2 and for the planning of activities to control events on levels of defence 3 and 4a as well as within the framework of accident management measures.

3 Technical criteria

3.1 Overall criteria

3.1 (1) In the design, manufacturing, construction and tests as well as during the operation and maintenance of the safety-relevant plant structures and components, principles and procedures are applied that are correspondence with the special safety-related requirements of nuclear technology. Upon the application of sound engineering practices, these are assessed case-by-case whether they comply with the state of the art in science and technology in the case of application.

3.1 (2) Safety-enhancing design, manufacturing and operating principles are applied to the measures and installations on levels of defence 1 to 3 with regard to all operating phases. In particular, the following are implemented:

a) safety margins in the design of components that are justified by safety engineering; here, established rules and standards may be applied with regard to the case of application;
b) use of qualified materials and of equipment that have been proven by operating experience or which have been sufficiently tested,
c) maintenance- and test-friendly design equipment, with special consideration of the radiation exposure of the personnel,
d) ergonomic design of the workplaces,
e) assurance and maintenance of the quality features during manufacturing, construction and operation,
f) performance of regular in-service inspections to an extent that is necessary from a safety-related point of view,
g) reliable monitoring of the relevant operating conditions in the respective operating phases,
h) preparation of a monitoring concept with monitoring systems to detect and control service- and ageing-induced damage,
i) recording, evaluation and safety-related use of the operating experience.

3.1 (3) In addition to subsection 3.1 (2), the following design principles are applied to the installations of level of defence 3 (safety installations) to ensure sufficient reliability:

a) redundancy,
b) diversity,
c) segregation of redundant subsystems, unless it is not conflicting with safety benefits,
d) physical separation of redundant subsystems;
e) safety-oriented system behaviour upon subsystem or plant component malfunctions;
f) preference of passive over active safety installations;
g) preference of principles of inherently safe design;
h) the auxiliary and supply systems of the safety installations are to be designed with such reliability that they ensure the required high availability of the installations to be supplied;
i) automation (in the accident analysis, installations that have to be actuated manually are in principle not considered until 30 minutes have passed).

3.1 (4) The required degree of redundancy of installations for ensuring safety functions depends on the safety significance in the defence-in-depth concept.

Safety installations are available redundantly and segregated in such a way that the safety functions are also sufficiently effective if it is postulated that, in the event of their required function,

- a failure of a safety installation due to a random single failure with the most unfavourable effects occurs, and
- generally there is at the same time an unavailability of a safety installation due to maintenance measures (maintenance case) with the most unfavourable effects in combination with a single failure.

N o t e: Further specifications are given in the “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 1.1 (Module 10).

3.1 (5) For active installations, single failures are always postulated and for passive installations generally postulated. Exceptions are justified.

N o t e: System- or component-specific specifications are given in the “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 1.1 (Module 10).

For passive installations, single failure is not postulated if it has been demonstrated that they fulfil the relevant requirements regarding design, construction, material selection, manufacturing, testability and operating conditions.

3.1 (6) If several installations have to fulfil their tasks simultaneously or subsequently for controlling a postulated case of challenge, occurrence of a single failure is postulated for the total of the installations but not in several of the installations required at the same time.

3.1 (7) Reliability and effectiveness of the measures and installations on level of defence 3, including the auxiliary and supply systems, are also ensured in the event of the required function

- under all conditions to be assumed for the event sequences,
- in the case of event-induced consequential failures,
- at the simultaneous or time-lag failure of the auxiliary power supply systems, and
- for failures according to the single-failure approach as outlined in subsection 3.1 (4).

3.1 (8) In the analysis of events on level of defence 3, it is generally assumed that no credit can be taken of the first actuation of the reactor protection system or the first actuation of reactor scram unless only one actuation criterion is available for physical and technical reasons.

Under the assumption that no credit can be taken of the first actuation, a single failure according to subsection 3.1 (4) is assumed to occur simultaneously in active system components, but not in case of simultaneous maintenance.

3.1 (9) In operating phases in which parts of the safety installations are scheduled to be unavailable, reliable and effective control is ensured under these conditions for the events to be assumed in these phases.

3.1 (10) In case of man-made hazards (level of defence 4a), process-related autarchy of the related emergency systems is ensured for at least 10 hours with respect to all cooling and operating agents necessary to take the plant to a controlled condition and maintain it in this condition.

The related emergency systems have no adverse safety-related effects on measures as well as installations of levels of defence 1 to 3.

3.1 (11) The planning of preventive and mitigative accident management measures is based on representative event sequences and phenomena. The preventive and mitigative accident management measures are effective for these representative event sequences and phenomena.

The installations provided for accident management measures neither affect operation as specified nor the deployment of safety installations and emergency systems in accordance with the design. The compatibility with the safety concept is ensured.

The accident management measures are oriented on the possible options provided by the plant concept.

3.1 (12) All safety-relevant installations are conditioned and arranged in such a way that they can be inspected and maintained in line with their safety significance and safety function prior to their commissioning and afterwards at regular intervals to a sufficient degree with regard to the determination of their specified condition and the detection of incipient deviations from verifiable quality features.

3.1 (12a) If for certain installations it is not possible to perform state-of-the-art in-service inspections to the extent necessary to detect possible deficiencies, it is ensured that

- for the areas with no or restricted testability, provisions are taken against failure resulting from potential damage mechanisms, such as fatigue, corrosion and other ageing mechanisms,
- a manufacturing documentation is available and no irregularities or deviations from requirements to be fulfilled are to be derived from it, and
- there are no findings from operation or according to the state of the art in science and technology for the parameters relevant here which raise concerns that safety-relevant damages may occur.

3.1 (12b) In the case of such restricted testability, measures and installations are provided for the control of the possible consequences of these deficiencies such to ensure compliance with the respective safety-related acceptance targets and acceptance criteria in the case of the events to be considered under these circumstances.

3.1 (12c) Combinations of postulated initiating events due to restricted testability with other postulated initiating events or the simultaneous failure of installations of the same type and installations subjected to the same loads with restricted testability are assumed unless it is shown that

- safety-relevant impairments of their condition and functions are excluded by the measures mentioned in subsection 3.1 (12b), or
- their simultaneous occurrence need not be assumed due to probability considerations or the state of the art in science and technology.

3.2 Criteria for the design of the reactor core and the shutdown systems

3.2 (1) On levels of defence 1 to 4a, the control of reactivity in the reactor core is ensured for all operating phases.

3.2 (2) The reactor core, the associated cooling systems and the relevant parts of the monitoring, control and limitation system as well as the reactor protection system and the installations for reactor shutdown are designed and constructed such and maintained in such a condition that

- on level of defence 1 the design limits, and

- on levels of defence 2 to 4a the respective applicable safety-related acceptance targets and acceptance criteria

are met.

3.2 (3) The reactor core is designed such that due to inherent reactor-physical feedback characteristics the fast reactivity increases are limited to such a degree that in combination with the other inherent characteristics of the plant and the shutdown systems the applicable safety-related acceptance targets and acceptance criteria are met on the respective levels of defence.

3.2 (4) The reactor core is designed such that due to inherent reactor-physical feedback characteristics the transients on level of defence 4a to be considered with postulated failure of the fast-acting shutdown system (reactor scram system) are limited to such a degree that in combination with other measures and installations of the plant, being effective as specified, the safety-related acceptance targets and acceptance criteria applicable for this event are met.

3.2 (5) The reactor has

- at least one system for fast shutdown (reactor scram system) by means of control elements (PWR) or control rods (BWR), and
- at least one more shutdown system, being independent of it and diverse, for reaching and long-term maintenance of subcriticality through injection of soluble neutron absorbers into the coolant.

The control and limitation system for the reactor power may totally or in part be identical with the shutdown systems as far as the effectiveness of the shutdown systems is maintained to the required degree at any time.

3.2 (6) The reactor scram system alone is able to bring the core into a subcritical state fast enough and keep it subcritical for a sufficiently long period

- from each condition on levels of defence 1 to 3, even if it is postulated that the most reactivity-effective control element or control rod is ineffective, and
- in case of man-made hazards conditions on level of defence 4a

so that the safety-related acceptance targets and acceptance criteria applicable on the respective levels of defence are met.

In case of events on level of defence 3, the postulated failure of the most reactivity effective control element or control rod may be treated as single failure according to subsection 3.1 (4) with regard to the subcriticality to be maintained.

3.2 (7) The reactor can be made subcritical and kept in a stable subcritical state on levels of defence 1 to 4a, even at the temperature, xenon concentration and the point in time of the cycle leading to the most unfavourable reactivity balance that is possible for the conditions and events to be considered.

For PWRs, the systems for injecting soluble neutron absorbers into the coolant alone are able to provide the required amount of subcriticality for the conditions and events of levels of defence 1 to 4a.

For BWRs, the following systems alone are able to provide the required amount of subcriticality:

- for conditions and event of levels of defence 1 to 4a, the electric motor-driven insertion of the control rods, and
- for conditions and events of levels of defence 1 and 2, the systems for injecting soluble neutron absorbers into the coolant.

N o t e: For the required amount of subcriticality, see “Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Core” (Module 2) and “Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors” (Module 3).

In case long-term maintenance of subcriticality on levels of defence 1 to 3 is ensured by the control rods alone, failure of the most effective control rod is postulated. On level of defence 3, this may be treated as single failure according to subsection 3.1 (4).

3.3 Criteria for the systems for fuel cooling

3.3 (1) Fuel cooling (heat removal from the reactor core) is ensured in all operating phases on levels of defence 1 to 4a.

3.3 (2) For this purpose, the heat produced in the fuel element is removed such that the safety-related acceptance targets and acceptance criteria for the fuel elements and the other safety-relevant installations applicable on the respective levels of defence are met during their entire operating life.

This is ensured by
a) availability of coolant and heat sinks to a sufficient degree, and
b) ensured heat transport from fuel to heat sink.

3.3 (3) Installations are available by means of which during normal and abnormal operation
a) the reactor can be started up and shut down reliably and according to the requirements, and
b) the heat can be removed reliably and according to the requirements also under consideration of all operating conditions during refuelling and, if required, the simultaneous cooling of the fuel elements in the fuel pool, as well as during maintenance measures.

3.3 (4) A reliable and redundant system for emergency cooling of the reactor core (emergency core cooling system) in case of a loss-of-coolant accident is provided that ensures for the break sizes, break locations, operating conditions and transients in the reactor coolant system to be considered that
a) the safety-related tasks are fulfilled, also with respect to the criteria of subsection 3.1 (4),
b) the respective applicable safety-related acceptance targets and acceptance criteria for the fuel elements, the core internals and for the containment are met.

3.3 (5) A reliable and redundant system for reactor shutdown and residual-heat removal in case of accidents without loss of coolant is provided which ensures that the safety-related acceptance targets and acceptance criteria are met even following an interruption or disturbance of heat removal from the reactor to the main heat sink, also with respect to the criteria of subsection 3.1 (4).

3.4 Criteria for the reactor coolant pressure boundary and the pressure-retaining walls of components of external systems

3.4 (1) The reactor coolant pressure boundary is designed, located and operated such that the occurrence of leaks that are not controlled by design, rapidly propagating cracks and brittle fracture need not be postulated.

3.4 (2) For this purpose, an adequate safety margin, justified from a safety point of view, is added in the design to the determined values of impacts according to the criteria of subsection 3.1 (2) to ensure that the design conditions of the reactor coolant pressure boundary are not exceeded. Further, measures and installations for the monitoring of causes and effects of damage mechanisms, in particular of leakages, during operation are specified and installed.

3.4 (3) For the reactor coolant pressure boundary and the pressure-retaining walls of components of external systems, basic safety is ensured by fulfilment of the following criteria under consideration of the operating medium:
- use of high-quality materials, in particular with regard to toughness and corrosion resistance,
- conservative limitation of stresses,
- prevention of stress peaks by optimised design and construction, and
- assurance of the application of optimised manufacturing and testing technologies.

This includes the knowledge and assessment of possibly existing defects.
N o t e: In case of the realisation of this basic safety, catastrophic failure of these plant components as a result of manufacturing defects is not postulated.

3.4 (4) For the reactor coolant pressure boundary and the pressure-retaining walls of components of external systems, leak and break postulates are defined within the framework of the design concept on level of defence 3. For piping systems and components of these systems for which catastrophic failure during plant operation is not postulated in the design concept and for which limited leak and break assumptions are made use of, there is a high validity regarding the impacts on these systems from levels of defence 1 to 4a.

For these selected piping systems and components it is demonstrated in addition that faults in the pressure-retaining walls cannot lead to a leak or break of the pipe or component which put the limited leak and break assumptions made use of into question. The compliance with the boundary conditions during operation considered here is verified.

3.4 (5) For preventing the excess of admissible pressure in the reactor coolant pressure boundary (for PWR plants including the secondary side of the steam generator), effective and reliable installations for pressure limitation and overpressure protection are provided.

Installations for depressurisation of the reactor coolant system are provided to perform accident management measures for depressurisation with a high degree of reliability.

3.4 (6) The nuclear power plant is operated such that the respective admissible values for impacts on the reactor coolant pressure boundary are not exceeded on levels of defence 1 to 4a. Here, the safety margins specified according to the criteria of subsection 3.1 (2) are considered.

3.5 Criteria for structures

3.5 (1) The structures are designed and kept in such a condition that they contribute to
- ensuring load transfer of the systems and components during operation and in the event of external or internal impacts,
- ensuring protection against these impacts,
- shielding of the ionising radiation and retention of radioactive materials, and
- fire and lightning protection of the plant

to the necessary extent.

3.6 Criteria for the containment

3.6 (1) The nuclear power plant has a containment which can fulfil its safety-related tasks under the operating conditions during which it is closed according to plan on levels of defence 1 to 3 and in case of transients with failure of reactor scram (level of defence 4a).

In operating phases during which the containment may be open according to plan, it is ensured that under the conditions of level of defence 1 and the events postulated on levels of defence 2 and 3, effective and reliable retention functions are available and an inadmissible release of radioactive materials from the containment is prevented or stopped in due time.

Components containing radioactive materials are installed within the containment system unless an inadmissible release of radioactive materials into the environment can be prevented otherwise in a sufficiently reliable manner.

Plant components under high pressure and containing reactor coolant are on principle installed inside the containment. An exception to this may be sections of the main steam lines and feedwater lines as well as other piping as far as this is technically required and as far as it is ensured that their rupture will not lead to any inadmissible radiation exposure in the environment.

Reliable, sufficiently fast and adequately long-lasting isolation of the containment penetrations is ensured.

3.6 (2) In case of a loss-of-coolant accident, a long-term temperature or pressure increase in the containment is prevented during sump operation.

3.7 Criteria for instrumentation and control

3.7 (1) The nuclear power plant is equipped with operational instrumentation and control installations on level of defence 1 that are designed and operated in such a manner that plant operation is ensured with as little disturbance as possible even without resorting to the installations provided on level of defence 2.

3.7 (2) The nuclear power plant is equipped with instrumentation and control installations with functions on level of defence 2 that are suitable for avoiding a challenge of the protective actions on level of defence 3 in case of events on level of defence 2.

3.7 (3) The nuclear power plant is equipped with reliable instrumentation and control installations with functions on level of defence 3 (reactor protection system) whose instrumentation and control functions initiate protective actions as soon as defined response levels are reached.

These installations are designed according to the following principles:
- redundant design of components, subassemblies and sub-systems,
- physical separation of installations corresponding to the impact range of possible postulated initiating events,
- diversity,
- automatic failure monitoring,
- adaptation of the components to the possible ambient conditions,
- simple software structure,
- limitation of the functional scope to the necessary safety-related degree,
- use of fault-preventing, fault-detecting and fault-controlling measures and installations.

3.7 (4) Monitoring and alarm installations are available at the nuclear power plant which on levels of defence 1 and 2 allow at any time a sufficient overview of the safety-related operating condition of the plant and the developing relevant processes to be able to register all safety-relevant operating parameters.

Alarm systems are available which indicate any changes in the plant operating condition that may result in a reduction of safety early enough to ensure that the corresponding safety-related acceptance targets are met.

3.7 (5) Specific accident instrumentation is available at the nuclear power plant which for event sequences and plant states on levels of defence 3 and 4
a) provides sufficient information about the plant condition to be able to take the necessary protective actions for the personnel and the plant or to initiate accident management measures and subsequently to determine their efficiency,
b) provides indications on the event sequence and allows its proper documentation,
c) allows an estimation of the effects on the environment.

3.7 (6) On levels of defence 4b and 4c, accident management measures are given priority over competing actions of the previous levels of defence. Interventions in equipment fulfilling instrumentation and control functions on levels of defence 1 to 4a are permitted if this is required by the accident management measures.

3.7 (7) The functions to be performed by instrumentation and control installations are classified by their safety-significance according to subsection 2.1 (10)). The criteria for the design, implementation, qualification, commissioning, operation and modification of the software and for the design, manufacturing, assembly and operation of the hardware (components, subassemblies and sub-systems) for instrumentation and limitation system are defined according to their safety-related classification.

3.7 (8) Unauthorised access to information systems and instrumentation and control installations of the plant is prevented. The effectiveness and reliability of the measures to be provided for this purpose corresponds to the safety significance of the information systems and instrumentation and control installations.

3.8 Criteria for control rooms

3.8 (1) A control room is available from where the nuclear power plant can be safely operated and from where measures can be taken in the event of an accident to maintain the nuclear power plant in a controlled and safe plant condition or take it to such a condition.

3.8 (2) A emergency control room is provided outside the control room from where in the event of a failure of the control room and rooms adjacent to it which have to be considered – such as the electrical distribution and switchgear room and the electronics room - the reactor can be shut down safely and kept subcritical, the residual heat can be removed, and the operating parameters relevant in this context can be monitored.

3.8 (3) The control room and the emergency control room are physically separated, independently power supplied and protected against external events in such a manner that they cannot be disabled at the same time.

3.8 (4) The ergonomic design of the control room and the emergency control room supports the safety-oriented behaviour of the personnel.

3.9 Criteria for the electrical energy supply

3.9 (1) The electrical energy supply of the nuclear power plant is designed such that on levels of defence 1 to 4a, the electrical energy supply of the consumers is ensured subject to their electrical supply conditions. The electrical energy supply is designed with such reliability that it will not be responsible for any unavailability of the systems to be supplied that might lead to adverse safety-related effects in case of their failure.

3.9 (2) For this purpose, a minimum of two largely independent grid connections for the power supply of the nuclear power plant are available. In addition to the electric power supply from the grid connections and the plant's main generator, reliable emergency power supply systems are provided for the plant's safety-relevant systems, ensuring the electric power supply of these systems in the event of a loss of preferred power and of the main generator. Furthermore, an electric power supply option exists ensuring independent of the power supply options mentioned above the electric power supply of at least one residual-heat removal chain including the necessary instrumentation and limitation system in the event of a failure of the grid connections.

3.9 (3) The necessary electric power supply for performing planned accident management measures is ensured.

3.10 Criteria for the handling and storage of the fuel elements

3.10 (1) On levels of defence 1 to 4a, the control of reactivity during fuel element storage is ensured for all operating phases.

3.10 (2) Measures and installations for the handling and storage of non-irradiated and irradiated nuclear fuel are provided such that a criticality event in the storage facilities is not to be postulated even under accident conditions or events on level of defence 4a.

3.10 (3) Fuel cooling (heat removal from the facilities for the storage of fuel elements) is ensured in all operating phases on levels of defence 1 to 4a

3.11 Criteria for radiation protection

3.11 (1) At the nuclear power plant, the personnel, organisational, spatial and equipment-related conditions are provided to ensure adequately precise and reliable radiation protection monitoring within the plant on all levels of defence to the necessary extent.

3.11 (2) At the nuclear power plant, the personnel, organisational and equipment-related conditions are provided to monitor and record the type, quantity and concentration of the radioactive materials to be discharged with the exhaust air and waste water with adequate precision and reliability to the necessary extent and to limit the discharge if necessary.

3.11 (3) The personnel, organisational and equipment-related conditions are provided to allow adequately fast, precise and reliable environmental radiation protection monitoring on levels of defence 1 to 4 to the necessary extent.

3.11 (4) Measures and installations are provided at the nuclear power plant that allow the safe handling, enclosure and storage of the non-irradiated and irradiated nuclear fuel or other radioactive material. These measures are designed such and these installations are in such a condition and located and shielded such that neither any inadmissible radiation exposure of the personnel and the environment nor any release of radioactive material into the environment need be assumed.

3.11 (5) The condition of nuclear power plants is such that they can be decommissioned in compliance with the radiation protection regulations. A concept exists for their removal after final decommissioning in compliance with the radiation protection regulations.

4 Postulated operating conditions and events

4.1 Operating conditions, anticipated operational occurrences and accidents

4.1 (1) The design of the measures and installations to be realised according to subsection 2.1 (3) on levels of defence 1 to 3 is based on:

- the operating conditions to be expected on level of defence 1, including testing conditions,
- the events whose occurrence is anticipated during the operating lifetime of the plant (level of defence 2), and
- a conservative spectrum of events whose occurrence is not to be expected during the operating lifetime of the plant due to the reliability and effectiveness of the measures and installations provided, but which have to be postulated in any case (level of defence 3).

4.1 (2) The respective measures and installations are designed such that it is demonstrated for the operating conditions and event sequences to be considered that the respective applicable safety-related acceptance targets and acceptance criteria are met, also considering specified boundary conditions.

4.1 (3) The completeness and the conservative character of the events to be considered are ensured plant specifically.

N o t e: The events at least to be referred to on the different levels of defence and the respective applicable safety-related acceptance targets and acceptance criteria to be met are presented in the “Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors” (Module 3).

4.1 (4) All installations required for the safe shutdown of the nuclear reactor, for keeping it in a shutdown state, for residual-heat removal or the prevention of a release of radioactive materials are designed such and constantly kept in such a condition that they can fulfil their safety-related tasks even in case of any natural impacts assigned to levels of defence 2 and 3, as far as they have to be considered, or other external events.

N o t e: Criteria for these installations to be considered with regard to malevolent disruptive acts or other third party intervention are not dealt with in the “Safety Criteria for Nuclear Power Plants”.

4.1 (5) The design of these installations is based on the following:

a) the respective natural impacts with the severest consequences or other external events to be considered at the site concerned;
b) the special characteristics of long-lasting external events;
c) combinations of several natural or other external events (e. g. earthquake, flood, storm, lightning, fires) or combinations of these impacts with internal events (e. g. pipe break, internal fires, smoke development, loss of offsite power); these combinations are postulated if the combined events may show a causal relationship or if their simultaneous occurrence has to be postulated according to probability considerations or according to the state of the art in science and technology.

4.1 (6) The foreseeable future development of the site properties regarding the external events to be considered has been taken into account.

4.1 (7) Fires and explosions at the plant are prevented. In addition, measures and installations exist to control fires. The safety-related measures as well as installations are designed and located such that the fulfilment of their tasks is not impaired inadmissibly by fires and explosions.

4.1 (8) Measures and installations are provided that prevent inadmissible consequences of plant-internal flooding.

4.1 (9) The different redundant sub-systems of safety installations are installed in physically separated locations or are protected such that a failure in more than one redundancy in case of any external or plant internal event (such as fire or flooding) need not be postulated.
N o t e: The events at least to be referred to on the different levels of defence and the respective applicable safety-related acceptance targets and acceptance criteria to be met are presented in the "Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors" (Module 3).

4.2 Man-made hazards

4.2 (1) In the design of the plant against external events, man-made impacts on level of defence 4a are also taken into account.

4.2 (2) The foreseeable future development of the site properties regarding the man-made hazard conditions to be considered is taken into account.

4.2 (3) Combinations of several external events allocated to level of defence 4a or combinations of these impacts with internal events (e.g. pipe break, internal fires, smoke development, loss of offsite power) are postulated if the combined events may show a causal relationship or if their simultaneous occurrence has to be postulated according to probability considerations or according to the state of the art in science and technology.

4.3 Events involving multiple failure of safety installations

4.3 (1) The planning of preventive accident management measures is based on a plant-specific spectrum of event sequences which comprises the following groups of events:
- transients,
- loss-of-coolant accidents inside the containment due to leaks in the reactor coolant system with an outflow surface of up to 0.1A of the cross-sectional area of the main coolant line,
- loss-of-coolant accidents with containment bypass.

Based on a multiple failure of safety installations, the representative event sequences to be referred to for the planning are defined.

4.4 Accidents involving severe core damage

4.4 (1) For the planning of mitigating accident management measures on level of defence 4c, a spectrum of events is postulated that takes the relevant phenomena of accidents with severe core damage into account for the respective plant type.

In this context, special attention is paid to those phenomena that put containment integrity at risk and which have an effect on the release of radioactive materials and on their possible release paths into the environment.

5 Criteria for documentation, operating rules and safety demonstration

5 (1) The licensee is in the position to provide documentary evidence on plant safety in a traceable manner.

5 (2) The licensee has available a systematic, complete, qualified and up-to-date documentation of the condition of the nuclear power plant.

5 (3) Written instructions exist for the safe operation of a plant, in which the following is specified:

a) A sufficiently complete set of provisions whose compliance ensures that the operation of the plant fulfils the safety requirements and conditions of the licence. The provisions comprise, in particular, the process-related and plant conditions, effectiveness, availability and relevant boundary conditions to be observed (operating limits and conditions).
   The specification of the operating limits and conditions is based on the plant design, the safety analyses, the licensing conditions and the experiences from commissioning and operation. The specification of the operating limits and conditions comprises all operating phases.
b) Instructions for the case of deviations from the operating limits and conditions.
c) The provisions to be fulfilled, performed and observed to prevent or control events on levels of defence 2 to 4a.
d) Severe accident management guidance (SAMG) as well as provisions for accident management measures and accident management guidelines applied within the framework of accident management.
e) The necessary in-service inspections of safety-relevant measures and installations.
f) The organisational regulations relevant for ensuring safe plant operation (structural and procedural organisation).
g) The minimum requirements on number and qualification of the personnel and the minimum availability of personnel at the plant for ensuring safe plant operation and control of events on levels of defence 2 to 4 under consideration of initiating events or consequential events, such as fire and / or occupational accidents.

5 (4) The documents according to subsection 5 (3) are kept updated. They are directly accessible to the personnel at the control room and the remote shutdown and control station.

5 (5) For update or amendment of the documents according to subsection 5 (3), a regulated procedure is provided which considers experience feedback and developments of science and technology.

5 (6) For all safety-relevant installations design codes, material specifications, assembly instructions and test codes as well as maintenance standards are provided or in place according to their safety relevance.

The test codes individually define qualification tests, material tests, structural inspections, pressure tests, acceptance tests and functional tests as well as in-service inspections.

Adherence to these instructions is monitored as part of a quality assurance programme. The results of the quality monitoring and the results of the tests are documented. The documents on the design, manufacture, construction and testings as well as on operation and maintenance of the safety-relevant installations that are necessary for assessing quality are accessible over the entire operating lifetime of the plant.

5 (7) The following deterministic and probabilistic methods may be applied to demonstrate that the technical safety criteria are met:

The deterministic methods comprise

a) the computational analysis of events and / or conditions,
b) the measurement and experiment, and
c) the engineering judgement.

The deterministic methods form the basis for the performance of system assessments.

5 (8) The safety demonstration is based on:

a) an up-to-date compilation of safety-relevant information about the current condition of the respective safety-relevant installations affected, also stating the tasks and safety functions to be performed on the different levels of defence, and about construction, layout, and design, and

b) a documented comparison of the actual condition of the safety-relevant installations affected with the licensed condition or the condition described in the licensing documents.

5 (9) For the analysis of events and conditions,

a) validated calculation methods are used for the respective scope of application,
b) any uncertainties associated with the calculation are quantified or considered by suitable methods.

5 (10) In case of findings that may put the validity of a safety demonstration into question, a review will be performed.

5 (11a) To supplement the deterministic safety analyses, the balance of the safety-related design is verified by probabilistic safety analyses (PSAs) in order to identify potential weak points.

5 (11b) To supplement the deterministic safety demonstrations, probabilistic safety analyses (PSAs) are applied to assess the safety significance

- of modifications of measures, installations or the operating mode of the plant, as well as
- new findings,

for which a significant influence on the PSA results cannot clearly be excluded.

5 (12) Measurements or experiments may be used for the safety demonstration if

a) the applicability of the experimental conditions to the plant conditions of the respective application context has been qualified, and
b) the uncertainties associated with the measurement have been quantified.

5 (13) Engineering judgement may be used for the safety demonstration if assessment criteria exist that are scientifically/technically reproducible.

B

MODULE 2
"Safety Criteria for Nuclear Power Plants: Criteria for the Design and Operation of the Reactor Core"

Contents

1 Objective

This guidance text contains safety-related criteria for the design and operation of the reactor core in a nuclear power plant.

N o t e: The guidance is structured into the design areas of nuclear, thermal-hydraulic and mechanical design. In addition, criteria for the design of the monitoring, control, limitation and shutdown systems as well as criteria for the reactor pressure vessel internals with regard to the assurance of safe shutdown and coolability of the core are presented. The criteria are allocated to the different levels of defence according to the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1), Section 2.1.

2 Scope

The criteria apply to the design and operation of the following reactor core components in nuclear power plants:

a) fuel rods,
b) fuel elements,
c) monitoring, control, limitation and shutdown systems.

The design and operation of the other core components are devised in a way that fulfilment of the criteria described below is not compromised.

N o t e: The acceptance targets and acceptance criteria to be fulfilled in the course of reactor design on level of defence 1 are presented in the following section.

A compilation of events on levels of defence 2 to 4a that have to be considered in the design of the core as well as of the respective safety-related acceptance targets and acceptance criteria to be fulfilled is contained in "Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors“ (Module 3).

Criteria for the handling and storage of core components, including criteria for refuelling, are compiled in the "Safety Criteria for Nuclear Power Plants: Criteria for the Handling and Storage of the Fuel Elements" (Module 11).

3 Criteria for nuclear design

(inherent safety, power and power density, reactivity changes)

3.1 Level of defence 1

3.1 (1) In the design of the nuclear core, all parameters are considered that influence the reactivity and power of the core or the power density as far as this is necessary for fulfilling the safety-related acceptance targets and acceptance criteria on the different levels of defence.

The dependencies of these parameters on the course of the cycle as well as the bandwidths of the admissible changes and fluctuations in the operating parameters under normal and abnormal operating conditions are taken into account.

3.1 (2) The reactor core is designed such that due to inherent reactor-physical feedback characteristics during normal operation and under the conditions of the events considered on levels of defence 2 to 4a,

a) fast reactivity increases are countered to such an extent that the respective safety-related acceptance targets and acceptance criteria applying to the different levels of defence are fulfilled in interaction with the other inherent characteristics of the plant and the shutdown systems;

N o t e: See also "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1), subsection 3.2 (3).

b) an increase in the fuel temperature in the reactor core leads to a negative reactivity effect;
c) an increase in the void content in the reactor core leads to a negative reactivity effect;
d) an increase in coolant temperature a n d / o r a decrease in coolant density in the reactor core leads to a negative reactivity effect,

– for PWRs at the latest upon reaching rated or partial load operation with xenon equilibrium at the beginning of the cycle, and
– for BWRs at the latest upon reaching operational temperature.

3.1 (3a) A positive reactivity effect upon an increase of coolant temperature or upon a decrease of coolant density (without or with negligible void formation) prior to reaching the conditions mentioned in subsection 3.1 (2d) is admissible if it can be shown that

– a stable control of reactor power is possible in this case under normal operating conditions and
– the respective safety-related acceptance targets and acceptance criteria are fulfilled if the resulting positive reactivity effects in connection with the events to be considered on levels of defence 2 to 4a are taken into account. For the analysis of transients with postulated failure

of reactor scram (level of defence 4a), subsection 3.2.5 (2) of the Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation (Module 6) is considered.

3.1 (3b) The safety relevance of increases of local void content, local coolant temperature increases or decreases of local coolant density with positive reactivity effects is assessed.

3.1 (4) The reactor core is designed and operated such that
a) power and power density as well as all safety variables that are relevant for reactivity, power or power density with regard to the fulfilment of the safety-related acceptance targets and acceptance criteria on the different levels of defence can reliably be monitored over time and space to the necessary extent;
   N o t e: For the definition of "monitoring", see "Safety Criteria for Nuclear Power Plants: Terms and Definitions".
b) power and power density distribution can be kept stable within permissible limits, also with regard to the effects of xenon redistributions;
c) changes in reactivity, power or power density take place in a controlled manner;
d) the reactor-physical boundary conditions that form the basis of the thermal-hydraulic and mechanical core design, the design of the control, limitation and shutdown systems and the design of the reactor pressure vessel and its internals are maintained.

3.1 (5) In the case of the BWR, precautions exist by the nuclear and the thermal-hydraulic design of the core that during normal operation there is a sufficient margin to the range in which undamped power density oscillations may occur (see also subsection 4.1 (3)).

3.1 (6) The design calculations regarding the reactor-physical safety variables of the core are checked by means of cycle-specific measuring programmes and by evaluating routine core monitoring data.
Specifications exist on how to proceed if significant deviations between calculation and measurement are observed.

3.2 Level of defence 2

3.2 (1) For the events considered on level of defence 2, the criteria for the design of the core components according to subsection 5.2 (1) as well as for the safety-related acceptance targets and acceptance criteria applying to level of defence 2 are met in interaction with the cooling systems and the measures and installations for limiting or reducing power or power density.

3.3 Level of defence 3

3.3 (1) For the events considered on level of defence 3, the safety-related acceptance targets and acceptance criteria applying to this level of defence are met.

3.4 Level of defence 4

3.4 (1) The reactor core is designed such that in case of an anticipated transient without scram (ATWS) (level of defence 4a), power is limited or reduced sufficiently fast due to a sufficiently negative reactivity effect in interaction with other measures and installations of the plant postulated to be effective so that the safety-related acceptance targets
a) maintenance of a reactor core geometry that can be shut down and cooled, and
b) maintenance of the integrity of the reactor coolant pressure boundary

and the acceptance criteria applying to these events are met.

By means of the other shutdown systems, the value of shutdown reactivity that is required for permanent subcriticality is achieved (see also subsection 6.4 (1)).

4 Criteria for thermal-hydraulic design

4.1 Level of defence 1

4.1 (1) The thermal-hydraulic core design considers all parameters that substantially influence the cooling of the fuel elements as far as this is necessary for fulfilling the safety-related acceptance targets and acceptance criteria.

The dependencies of these parameters on the course of the cycle as well as the bandwidths of the possible changes and fluctuations in the operating parameters under normal and abnormal operating conditions are taken into account.

4.1 (2) The reactor core is designed and operated such that

a) all safety variables that are relevant for the cooling of the fuel elements with regard to the fulfilment of the safety-related acceptance targets and acceptance criteria on the different levels of defence can reliably be monitored over time and space to the necessary extent;
b) a critical boiling condition will not occur;
c) the thermal-hydraulic boundary conditions that form the basis of the nuclear and mechanical core design, the design of the control, limitation and shutdown systems and the design of the reactor pressure vessel and its internals are maintained.

4.1 (3) In the case of the BWR, precautions exist by the nuclear and the thermal-hydraulic design of the core that during normal operation there is a sufficient margin to the range in which undamped power density oscillations may occur (see also subsection 3.1 (5)).

4.1 (4) The design calculations regarding the thermal-hydraulic safety variables of the core are checked by means of cycle-specific measuring programmes and by evaluating routine core monitoring data.
Specifications exist on how to proceed if significant deviations between calculation and measurement are observed.

4.2 Level of defence 2

4.2 (1) For the events considered on level of defence 2, the criteria for the design of the core components according to subsection 5.2 (1) as well as for the safety-related acceptance targets and acceptance criteria applying to level of defence 2 are met in interaction with the cooling systems and the measures and installations for limiting or reducing power or power density.

4.3 Level of defence 3

4.3 (1) For the events considered on level of defence 3, the safety-related acceptance targets and acceptance criteria applying to this level of defence are met.

4.4 Level of defence 4

4.4 (1) For level of defence 4, there are no criteria for the thermal-hydraulic design of the reactor core beyond those mentioned in Section 3.4.

5 Criteria for mechanical design

5.1 Level of defence 1

5.1 (1) The mechanical design of the core components takes into account all mechanical, thermal, chemical and radiation-induced impacts on the core components that are relevant with respect to the fulfilment of the criteria according to Annex 1 to Annex 3 as well as to the safety-related acceptance targets and acceptance criteria. The dependencies of these impacts on the course of the cycle have been considered.

5.1 (2) The core components and the reactor cores assembled from it are designed and operated such that the required operability of the core components is ensured according to the design until the end of their operating time.

The compatibility of the core components is ensured.

In particular it is ensured that there will be no deformation of the fuel rods, the fuel element structure, the control elements (PWR) or control rods (BWR) that jeopardises the ability of mechanical shutdown a n d / o r the coolability of the core.

5.1 (3a) For the fuel rods, design limits pertaining to the criteria of a) to j) listed in Annex 1 are defined. These limits may be fuel- or material-specific.

5.1 (3b) Alternatively to the design limits mentioned in subsection 5.1 (3a), experimentally substantiated failure probabilities may be defined.

5.1 (4) As regards the fuel element structure, design limits pertaining to the criteria listed in Annex 2 are defined and met; these design limits may be design- and material-specific.

5.1 (5) As regards the control elements or control rods, design limits pertaining to the criteria listed in Annex 3 are defined and met; these design limits may be design- and material-specific.

5.1 (6) The design limits according to subsections 5.1 (3a), 5.1 (4) and 5.1 (5) are defined such – with consideration of the uncertainties attached to the experimental database – that defects on the fuel rods, fuel element structures or on the control elements or control rods as well as on the structural parts pertaining to them need not be postulated if the design limits are met.

5.1 (7) When demonstrating fuel rod integrity, it is shown that the design criteria stated in Annex 1 are met. It is shown that

a) if demonstrations are done by means of deterministic methods, no fuel rod will exceed the design limits according to subsection 5.1 (3a) during its operation time
b) if demonstrations are done by means of statistical methods, the probability that not more than one fuel rod per cycle will exceed the design limits according to subsection 5.1 (3) is at least 95% with a minimum confidence level of 95%.

   When using failure probabilities according to subsection 5.1 (3b) it is shown that the probability that no fuel rod per cycle will fail is at least 95% with a minimum confidence level of 95%.

   N o t e: See also “Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation” (Module 6), subsection 3.3 (4).

5.1 (8) The fuel elements are designed such that inspections of the fuel rods and of the fuel element structure with regard to their required operating behaviour are possible.

5.1 (9) Tests of the fuel elements as well as of the control elements or control rods with regard to their required operating behaviour are performed.

5.1 (10) The materials used in the reactor core are compatible with the water chemistry of the reactor coolant so that any inadmissible changes of surfaces in the reactor core due to corrosion and deposits is prevented.

5.2 Level of defence 2

5.2 (1) For the events on level of defence 2, the unrestricted further use and ability of handling of the fuel elements as well as of the control elements (PWR) or control rods (BWR) is ensured. The design limits according to subsections 5.1 (4) and 5.1 (5) as well as the criteria of subsection 5.1 (7) are met.

It is ensured in particular that no deformation of the fuel rods, the fuel element structure, the control elements or control rods occurs as a result of events on level of defence 2 that jeopardises the ability of mechanical shutdown a n d / o r the coolability of the core.

5.3 Level of defence 3

5.3 (1) For the events considered on level of defence 3, the safety-related acceptance targets and acceptance criteria applying to this level of defence are met.

It is ensured in particular that no deformation of the fuel rods, the fuel element structure, the control elements or control rods occurs as a result of an event on level of defence 3 which jeopardises

- the ability of mechanical shutdown (permanent shutdown in the case of a large break accident in a PWR) and / or
- the coolability of the core.

5.3 (2) The effects of the changes in the properties of the fuel rods, the fuel element structure, and the control elements or control rods due to normal and abnormal operation on their accident behaviour are taken into account.

5.4 Level of defence 4

5.4 (1) For level of defence 4, there are no criteria for the mechanical design of the reactor core beyond those mentioned in Section 3.4.

6 Criteria for the design of the monitoring, control, limitation and shutdown systems

6.1 Level of defence 1

6.1 (1) Operation of the reactor core is monitored as follows:

a) Power and power density as well as all safety variables that are relevant for reactivity, reactor power, the power density and the cooling of the fuel elements with regard to meeting the safety-related acceptance targets and acceptance criteria are reliably monitored over time and space to the necessary extent.
b) The spatial distribution as well as the sensitivity and the implemented design of the monitoring devices ensure the respective necessary functions of the control, limitation and safety systems under all operating conditions of the plant as well as in case of events on levels of defence 2 to 4a.
c) It is ensured that all set points of the control, limitation and safety systems are defined and set with consideration of the respective operating conditions and the core design so that function of the control, limitation and safety systems as designed is reliably ensured.
d) It is ensured that by means of the directly measured values, the derived safety-relevant parameters can be reliably determined, too.
e) It is ensured that those safety variables of the reactor core that have an influence on the safety demonstration on levels of defence 2 to 4a are kept within the bandwidth for which it has been shown that the respective events are controlled

6.1 (2) Power and power density are kept within permissible limits in such a way that the nuclear, thermal-hydraulic and mechanical design criteria (according to Sections 3.1, 4.1 and 5.1) are also met under consideration of the changes in the parameters with an effect on reactivity that may occur during normal operation.

6.1 (3) The design of the control, limitation and shutdown systems takes into account all mechanical, thermal, chemical and radiation-induced impacts that may occur during the operation of the plant or with regard to control, limitation and shutdown systems whose proper functioning is required to control events on levels of defence 2 to 4a, even under the corresponding conditions of the respective events.

6.1 (4) The design of the control, limitation and shutdown systems takes into account all parameters that influence the effectiveness of these systems.

6.1 (5) The reactor scram system according to subsection 3.2 (5) and 3.2 (6) of the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1)

a) is automatically triggered by actuators that are formed by different process variables according to the criteria for instrumentation and control functions of Category A (see "Safety Criteria for Nuclear Power Plants: Criteria for Instrumentation and Control and Accident Instrumentation“ (Module 5) subsection 5 (2));

b) will not be impaired in its specified function (not even by a function generated by a fault in these systems) even in case that it shares common components with the control or limitation systems by the function of the control or limitation system;
c) can also be triggered manually.

6.1 (6) The shutdown systems according to subsection 3.2 (7) of the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1) ensure that the amount of shutdown reactivity required is reached and can be maintained for a limitless period.

For BWRs, the systems for the injection of soluble neutron absorbers into the coolant provide an amount of shutdown reactivity of 5% in operating phases A to C.

6.1 (7) The reliability and effectiveness of the systems and components relevant to the shutdown is ensured by their design and by regular tests as well as by suitable maintenance measures over their entire operating time. Here, the following applies in particular:
a) Periodically, all control elements or control rods are checked with regard to proper manoeuvrability.
b) The proper function of the reactor scram system is shown at the end and before the beginning of a cycle as well as after each reactor scram. In addition, proper function of components concerned is checked after each maintenance measure which may impair the operability of reactor scram..
c) If a control element or control rod can be moved no more or only with high forces or if delayed drop or fast insertion times are identified, the circumstances will immediately be assessed from a safety-related point of view (ensuring the necessary limitation and shutdown functions, maintenance of shutdown reactivity, possibility of a common-mode failure). If safe continued operation cannot be guaranteed any longer without doubt, the reactor is rendered subcritical. If damage to the control elements or control rods have caused the strong forces, these components are replaced or repaired.
d) The drives of the control elements or control rods including all associated auxiliary systems only share the same components if it is ensured that a single failure will not impair reliable and effective shutdown of the reactor.
e) Measures and installations are provided to prevent the uncontrolled withdrawal of control elements or control rods.
f) For BWRs, it is ensured that after a shut-off of all forced circulation pumps there will be no start of forced circulation pumps if control rods are withdrawn.
g) For shutdown systems working with boron injection, periodic as well as case-specific monitoring of the boron concentration and the fill level in the storage tanks important to safety are provided in a way that ensures boron injection as required.
h) Shutdown of the reactor is also ensured even if several events that are not independent of each other occur (e.g. fire, internal flooding).

6.2 Level of defence 2

6.2 (1) Automatic installations for limiting or reducing power or power density are provided which in interaction with the nuclear, thermal-hydraulic and mechanical design of the reactor core ensure that
- a potential reactivity addition and related possible increase of reactor power or power density, and
- degradation of fuel element cooling

as a result of events on level of defence 2 are limited to such an extent that the safety-related acceptance targets and acceptance criteria of this level of defence are fulfilled.

6.2 (2) For transients that are to be expected during the reactor's operating time and during which changes in operating parameters are generated at such magnitudes that reactor scram will occur, the reactor scram system ensures that the required amount of shutdown reactivity will be reached in accordance with the criteria of subsection 3.2 (6) of the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1) such fast that the safety-related acceptance targets and acceptance criteria applying on level of defence 2 are fulfilled.

6.2 (3) In the events considered, the reactor scram keeps the reactor in subcritical condition until permanent maintenance of subcriticality is ensured.

6.2 (4) The shutdown systems according to subsection 3.2 (7) of the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1) ensure that for events on level of defence 2, the amount of shutdown reactivity required is reached and can be maintained for a limitless period.

6.2 (5) The effectiveness and motion speed of both individually and jointly moving control elements or control rods as well as of other installations influencing reactivity levels are limited such that the safety-related acceptance targets and acceptance criteria of level of defence 2 are fulfilled even in the event of an erroneous moving command.

6.2 (6) If a rise in the local power density due to a redistribution of the neutron flux caused by an operational disturbance cannot be precluded, measures and installations are provided for an effective limitation of this rise.

6.2 (7) For the BWR it is ensured by effective and reliable automatic measures that power density oscillations that may occur in case of leaving the stable range of the operating map due to an operational disturbance, undamped oscillations are prevented or stopped in good time so that the safety-related acceptance targets and acceptance criteria on level of defence 2 are fulfilled.

6.3 Level of defence 3

6.3 (1) The reactor scram system ensures for the relevant events on level of defence 3 that in accordance with the criteria of subsections 3.1 (8) and 3.2 (6) of the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1) the required amount of shutdown reactivity is reached in interaction with other safety systems such fast that the safety-related acceptance targets and acceptance criteria applying on level of defence 3 are fulfilled.

6.3 (2) In the events considered on level of defence 3, the reactor scram keeps the reactor in subcritical condition until permanent maintenance of subcriticality is ensured.

6.3 (3) For the PWR, notwithstanding subsection 6.3 (2), a short return to criticality is permissible in events involving fast cool-down of the reactor core (subcooling transients, see "Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors“ (Module 3)) if fulfilment of the otherwise applicable acceptance criteria is ensured.

6.3 (4) The shutdown system according to subsection 3.2 (7) of the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1) ensure that for events on level of defence 3, the amount of shutdown reactivity required is reached and can be maintained for a limitless period.

6.3 (5) The installations necessary for forced speed reduction to minimum value of the recirculation pumps of a BWR are designed as I&C installations for the fulfilment of instrumentation and control functions of Category A according to the "Safety Criteria for Nuclear Power Plants: Criteria for Instrumentation and Control and Accident Instrumentation (Module 5).

6.3 (6) Apart from the safe design and thorough in-process inspections as well as apart from specific interlocks (BWR), further independent measures and installations are provided to prevent the complete ejection of a control element or control rod or a control rod (BWR) unless it has been demonstrated that in the event of the ejection of a control element or control rod or the drop of a control rod with the highest reactivity value the safety-related acceptance targets and acceptance criteria are fulfilled.

6.3 (7) The effectiveness and motion speed of both individually and jointly moving control elements or control rods as well as of other installations influencing reactivity levels are limited such that the safety-related acceptance targets and acceptance criteria of level of defence 3 are fulfilled in the event of an accident resulting from erroneous activation of these installations.

6.4 Level of defence 4

6.4 (1) For events of level of defence 4a, the required amount of shutdown reactivity is reached by the respectively available shutdown systems in accordance with the criteria of above subsection 3.4 (1) as well as subsections 3.2 (6) and 3.2 (7) of the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1) and maintained for a limitless period.

7 Criteria for the design of the reactor pressure vessel internals

N o t e: In the following, the reactor pressure vessel internals are understood to be in particular:

in a PWR:
-the upper and lower core structure

in a BWR:
-the core shroud
-the upper and lower core lattice
-control rod guide tubes
-steam-moisture separator
-steam dryer
-feedwater distributor.

7.1 Level of defence 1

7.1 (1) In the design of the reactor pressure vessel internals, all mechanical, thermal, chemical and radiation-induced impacts are considered that may occur during the operation of the plant as well is in events on levels of defence 2 to 4a.

7.1 (2) The reactor pressure vessel internals withstand all loads occurring during normal operation over their entire operating time in such a way that normal operating conditions of the reactor core are ensured.

7.1 (3) Suitable measures and installations are provided to prevent that reactivity control or fuel cooling is impaired by impurities or loose parts in the coolant.

7.1 (4) The vibration behaviour of the reactor pressure vessel internals is studied by way of measurements during first commissioning of the plant. Measures and installations for operational monitoring are provided to the extent required for reasons of safety.

7.1 (5) Tests of the reactor pressure vessel internals are provided with regard to the occurrence of damage and to ensure their required operability.

7.2 Level of defence 2

7.2 (1) The reactor pressure vessel internals are designed such that in case of events on level of defence 2 and the resulting impacts on the internals, it is ensured that the safety-related acceptance targets and acceptance criteria of this level of defence are fulfilled.

7.3 Level of defence 3

7.3 (1) The reactor pressure vessel internals are designed such that in case of events on level of defence 3 and the resulting impacts on the internals, it is ensured that the safety-related acceptance targets and acceptance criteria of this level of defence are fulfilled.

It is ensured in particular that the ability of mechanical shutdown (permanent shutdown in the case of a large break accident in a PWR) and coolability of the core is maintained for events of level of defence 3.

N o t e: See "Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors" (Module 3) Annex A2 on the scope of safety demonstration regarding leaks larger than 0.1 A.

7.4 Level of defence 4

7.4 (1) The reactor pressure vessel internals are designed such that in case of events on level of defence 4a and the resulting impacts on the internals, the safety-related acceptance targets and acceptance criteria of this level of defence are met.

Annex 1

Design criteria for fuel rods

For the fuel rods, the following design criteria apply:

a) prevention of fuel melting,
b) limitation of the total hoop strain of the cladding due to fast power increase,
c) limitation of stress cycles fatigue upon dynamic loading,
d) limitation of the pressure difference across the cladding as a result of outer overpressure,
e) limitation of stresses in the free-standing cladding,
f) limitation of inner fuel rod pressure to prevent inadmissible thermal feedback,
g) limitation of the cladding tensile plastic equivalent strain ,
h) limitation of the thickness of the cladding oxide layer,
i) limitation of hydrogen uptake into the cladding (with consideration of the distribution of the hydrogen uptake in the cladding),
j) limitation of hoop stress in the cladding (with consideration of hydride orientation),
k) limitation of fretting,
l) fuel rod damage due to mechanical-chemical interactions between fuel and cladding (PCI/SCC) is prevented by the design of the fuel rods a n d / o r by proper operation of the reactor core.

The above-mentioned design criteria apply to the design concepts currently in use. If other designs are employed, different design criteria are applied if necessary which have been confirmed to be equally suited for ensuring fulfilment of the overall safety-related criteria.

Annex 2

Design criteria for the fuel element structure

For the fuel element structure, the following design criteria apply:

a) prevention of fuel element lift-off from the lower core support plate through sufficient hold-down force on the fuel element or through the limitation of the buoyancy force to admissible values,
b) limitation of stresses within the control element guide tubes to prevent inadmissible deformation (PWR),
c) limitation of compressive stresses within the control element guide tubes to prevent buckling (PWR),
d) limitation of equivalent stresses within the structural components of the fuel elements,
e) limitation of stress cycles of the fuel element structural components to prevent fatigue,
f) limitation of fretting at contact points of the fuel element structural components with movable design parts,
g) limitation of compressive stresses on the fuel rod which result from fixation forces of the spacer grids,
h) prevention or limitation of compressive stresses within the fuel rod occurring due to fuel rod growth upon filling the fuel rod free space (PWR: prevention through sufficient axial free space, BWR: preventing the axial spring from being fully compressed),
i) prevention of compressive stresses within the fuel element occurring due to fuel element growth upon filling the fuel element free space (prevention through sufficient axial free space),
j) limitation of embrittlement in the fuel element structure through limitation of the hydrogen uptake in the fuel element structure,
k) limitation of spring relaxation,
l) limitation of the differential growth of the different fuel element components,
m) limitation of the stresses within the water-bearing structure of the fuel elements (e.g. fuel element channel wall, water channel) (BWR),
n) limitation of the deformation of water-bearing structure of the fuel elements (BWR).

The above-mentioned design criteria apply to the design concepts currently in use. If other designs are employed, different design requirements are applied if necessary which have been confirmed to be equally suited for ensuring fulfilment of the overall safety-related criteria.

Annex 3

Design criteria for control elements and control rods

For control elements and control rods, the following design criteria apply:

a) limitation of maximum pressure loading,
b) limitation of the (equivalent) stresses in the absorber cladding as well as in the other structural components,
c) limitation of the absorber material temperature,
d) limitation of absorber cladding fatigue and fatigue of other structural components upon load change,
e) limitation of equivalent plastic strain of the absorber cladding and the other structural components,
f) provision of sufficient absorption effect for the scheduled operating time.

The above-mentioned design criteria apply to the design concepts currently in use. If other designs are employed, different design requirements are applied if necessary which have been confirmed to be equally suited for ensuring fulfilment of the overall safety-related criteria.

C

MODULE 3
"Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors"

Contents

1 Objectives and scope

1 (1) For the events presented in the following generic event lists for PWRs and BWRs (hereinafter referred to as event lists), it is demonstrated that the criteria specified in the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria” (Module 1) have been met. Especially for these events it is demonstrated in accordance with the “Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation“ (Module 6) that the safety-related acceptance targets and acceptance criteria applicable on the different levels of defence in depth are achieved and maintained. In this respect, it is assumed that the requirements for integrity, effectiveness, function and reliability of components, structural plant components or other plant equipment used and for their support stability are fulfilled.

N o t e: In the event lists, the events are classified according to the respective protection goals

- control of reactivity (R),
- cooling of the fuel elements (K), and
- confinement of radioactive material (B).

Those events that are of importance for demonstrating that the radiological safety objectives have been met are classified as (S).

For each protection goal, the acceptance targets and criteria assigned to the levels of defence 2 to 4a are presented in the Tables 3.1a-c for the reactor plant and in Table 3.2 for fuel element storage and handling, for the radiological safety objective in Table 3.3. For events which are counteracted by design requirements for construction and operation of the plant, the event lists do not show specifically concerned protection goals but reference is made to the respective design requirements in the “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components” (Module 10), Section 2 and 3. The primary objective for these events is to prevent impacts due to internal and external events that concern more than one redundancy.

For defined events, there is the option of demonstrating that the occurrence of these events is so unlikely due to preventive measures that it does not have to be postulated. In the event lists, these are referred to with “VM” (Vorsorgemaßnahmen). General and, where appropriate, event-specific criteria for these preventive measures are included in “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 4 (Module 10).

1 (2) The fulfilment of the criteria according to 1 (1) is demonstrated on the basis of the operating phases defined in the following:

- Operating phase A
  Power operation via main heat sink. This operating phase covers all load conditions of the plant.
- Operating phase B
  Startup of the plant or shutdown via main or auxiliary heat sink.
- Operating phase C
  Residual-heat removal operation with the nuclear residual-heat removal system; primary system or reactor coolant system pressure-tight closed.
- Operating phase D
  Residual-heat removal operation with the nuclear residual-heat removal system; primary system or reactor coolant system not pressure-tight closed; reactor cavity or reactor internals storage pool not or only partly flooded.
- Operating phase E
  Residual-heat removal operation; reactor cavity or reactor internals storage pool completely flooded.
- Operating phase F
  Fuel element cooling; core completely unloaded and fuel pool separated from reactor cavity or reactor internals storage pool.

N o t e: The classifications (start and end) of the above-mentioned operating phases for PWRs and BWRs are presented in Tables 4.1 to 4.3.

Where other operating phase definitions are chosen in the plant operating procedures than those mentioned in subsection 1 (2), the event lists and the acceptance targets and acceptance criteria assigned to the events are adapted accordingly.

1 (3) For events whose occurrence does not have to be postulated if special measures and facilities are provided – in the following referred to as preventive measures – it is demonstrated that the criteria for effectiveness and reliability of the respective preventive measures are fulfilled.

2 General criteria

2 (1) As far as plant-specific conditions require deviations from the boundary conditions - specified in the event lists - in the analyses for safety demonstrations, deviations shall be justified and documented in a comprehensible way.

2 (2) If in the safety demonstrations only some aspects of the respective event list are of significance, the safety demonstrations may be limited to the aspects concerned.

2 (3) The safety demonstrations cover the period from event occurrence until reaching a controlled plant condition; for determination of a source term for radiological safety analyses, the period lasts until the end of the release.

2 (4) For the plant-specific application of the event lists, the completeness and representative character of the events mentioned in the lists have been checked for levels of defence 2 to 4a for all relevant operating conditions.
In this respect, the following working steps were generally taken:
a) Comparison of the events investigated in connection with construction, operating and modification licences and safety reviews pursuant to §19a of the Atomic Energy Act (AtG) with the events summarised in the event lists (Tables 5.1 to 5.3).
b) Verification of the representative character of the event lists and – where required – plant-specific supplementation and adjustment of the lists.
c) As far as appropriate for level of defence 2, condensing of the event lists prepared according to b) under the aspect of the representative character of individual events. Condensing is justified in a detailed and comprehensible manner.
d) Demonstration of fulfilment of the relevant acceptance criteria and of the general criteria for all events of the event lists prepared under consideration of steps b) and c).

2 (5) The verifications of fulfilment of the acceptance criteria consider the classification of load levels of the reactor coolant pressure boundary, the external systems and the containment according to the events included in the event lists, presented in Annex 1.

3 Acceptance targets and acceptance criteria

Table 3.1a: Safety-related acceptance targets and acceptance criteria of levels of defence 2 to 4a for the reactor plant and the protection goal “control of reactivity”

Level of defence:	**2**					**3**					**4a**
Operating phase:	**A**	**B**	**C**	**D**	**E**	**A**	**B**	**C**	**D**	**E**	**A – E**
Protection goal:	**Control of reactivity (R)**										
Acceptance targets:	**Power adjustment or reactor shutdown** [1]					**Reactor shutdown** [a)]					
Acceptance criteria:	Also see “Cooling of the fuel elements“ and “Confinement of radioactive material “										
Acceptance target:	**Ensuring subcriticality**										
Acceptance criterion[2] **“Amount of shutdown reactivity”:**	≥ 1 %	≥ 1 %	PWR: ≥ 5 % BWR: ≥ 1 %			≥ 1 %					≥ 1 %

[1] Only operating phase A and with regard to reactor shutdown for BWRs also temporarily in operating phase E during refuelling.

[2] Acceptance criteria for the effectiveness of reactor scram (only operating phase A and for BWRs also temporarily in operating phase E during refuelling) and shutdown in the long term (all operating phases). The boundary conditions specified in the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria” (Module 1), subsections 3.2 (6) and 3.2 (7) and the ”Safety Criteria for Nuclear Power Plants: Criteria for the Design and Operation of the Reactor Core“ (Module 2), subsections 6.2 (2), 6.2 (4), 6.3 (1) and 6.3 (4) have been met.
For refuelling (operating phase E, BWR), failure of fast insertion of the most effective control rod was not postulated.

Table 3.1b: Safety-related acceptance targets and acceptance criteria of levels of defence 2 to 4a for the reactor plant and the protection goal "cooling of the fuel elements"

Level of defence:	2					3					4a	
Operating phase:	**A**	**B**	**C**	**D**	**E**	**A**	**B**	**C**	**D**	**E**	**A – C**	**D – E**
Protection goal:	**Cooling of the fuel elements (K)**											
Acceptance targets:	**Unrestricted reuse of the fuel elements**[3]					**Possibility of shutdown and cooling of the reactor core**					**Possibility of shutdown and cooling of the reactor core**	
Acceptance criteria:	- $T_{Fuel} < T_{Melt}$ [4] - No critical boiling at cladding tube or maintenance of an appropriate temperature-time criterion of the cladding tube			No boiling at the cladding tube		<u>Transient:</u> Fuel rod integrity [5] <u>Reactivity accident:</u> Fuel remains within the cladding tube [6] <u>LOCA:</u> - fuel rod integrity (if leak ≤ 0.1 A) -Cladding tube temperature < 1200 °C [7] -Cladding tube oxidation depth < 17 % d -Limitation of cladding tube expansion [8]			Fuel rod integrity (maintenance of fuel coverage)		<u>Transient with postulated scram failure:</u> (operating phase A) Ability of mechanical shutdown in the long term and cooling <u>Man-made hazard conditions:</u> (operating phase A-C) Ability of mechanical shutdown (only A) and fuel rod integrity	Fuel rod integrity[9]

[3] The acceptance criteria also to be referred to for ensuring unrestricted reuse within the framework of the design of fuel elements and other core internals are state in "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Operation of the Reactor Core" (Module 2), subsection 5.2 (1)

[4] Fuel melting temperature in the hot rod under consideration of the radial power distribution in the pellet not reached.

5 No critical boiling at the fuel rod cladding tubes or maintenance of an appropriate temperature-time criterion.

[6] A preceding acceptance criterion for this concern is the integrity of the cladding tube. The integrity of the cladding tube is ensured if the maximum enthalpy release in the fuel (radially averaged over the pellet cross section) remains below a cladding tube damage limit depending on material condition and burn-up.

[7] By fulfilment of the acceptance criteria, the following is ensured:

- Maintenance of a residual ductility of the cladding tube under consideration of the transient and, where applicable, also two-sided oxygen and hydrogen uptake into the cladding tube so that a fragmentation of the cladding tube due to the event and the following handling actions does not occur. Definition of cladding tube oxidation depth: equivalent part of the cladding tube wall consumed by oxidation. Amount of consumed cladding wall is calculated here according to "L. Baker Jr., W. C. Just, Studies of Metal-Water-Reactions of High Temperatures III, Experimental and Theoretical Studies of the Zirconium-Water-Reaction, ANL-6548, 1962".
- Prevention of reaching temperature conditions under which the zirconium-water reaction is autocatalytical.

Applicability of this criterion combination for achievement of these acceptance targets was demonstrated for the respective cladding tube materials used and the expected initial cladding tube conditions.

[8] Maintenance of a conduit which ensures sufficient cooling of the fuel rods.

[9] As far as accessibility of the containment or the reactor building is required for maintenance of fuel element cooling, it is demonstrated that the conditions for accessibility are fulfilled.

Table 3.1c: Safety-related acceptance targets and acceptance criteria of levels of defence 2 to 4a for the reactor plant and the protection goal “confinement of radioactive material”

<table>
<tr><td colspan="2">Level of defence:</td><td colspan="5">2</td><td colspan="5">3</td><td colspan="3">4a</td></tr>
<tr><td colspan="2">Operating phase:</td><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>A – B</td><td>C</td><td>D – E</td></tr>
<tr><td colspan="2">Protection goal:</td><td colspan="13">Confinement of radioactive material (B)</td></tr>
<tr><td colspan="2">Acceptance target:</td><td colspan="13">Maintenance of barrier integrity</td></tr>
<tr><td rowspan="9">Acceptance criteria</td><td rowspan="2">Fuel rod cladding tube:</td><td colspan="13">See “Cooling of the fuel elements“</td></tr>
<tr><td>PCI [a]</td><td colspan="4">-</td><td colspan="2">LOCA > 0.1 A:
Fuel rod damage extent ≤ 10 %</td><td colspan="3">-</td><td colspan="3">-</td></tr>
<tr><td>Reactor coolant pressure boundary:</td><td colspan="5">See Annex 1</td><td colspan="5">See Annex 1</td><td colspan="3">See Annex 1</td></tr>
<tr><td>External systems</td><td colspan="5">See Annex 1</td><td colspan="5">See Annex 1</td><td colspan="3">See Annex 1</td></tr>
<tr><td rowspan="3">Containment:</td><td colspan="3">Pressure increase in the containment < response criteria reactor protection</td><td colspan="2" rowspan="2">-</td><td colspan="3">$P_{cont.} \leq P_{cont.-A}$ [b]</td><td colspan="2" rowspan="2">-</td><td>$P_{cont.} \leq P_{cont.-A}$ [c]</td><td colspan="2" rowspan="2">-</td></tr>
<tr><td colspan="3">BWR: Maintenance of specified temperatures in the wetwell</td><td colspan="3">BWR: Maintenance of specified temperatures in the wetwell
Limitation of
-zirconium-water reaction to < 1 % of the total zirconium contained in the reactor core
-max. local H_2 concentration in the containment to values below the ignition value</td><td>BWR: Maintenance of specified temperatures in the wetwell</td></tr>
<tr><td colspan="5">See Annex 1</td><td colspan="5">See Annex 1</td><td colspan="3">See Annex 1</td></tr>
<tr><td>Acceptance target:</td><td colspan="13">Maintenance of retention function of systems</td></tr>
</table>

<table>
<tr><td colspan="2">Acceptance criteria:</td><td colspan="5">see under
“Achievement of the radiological safety objectives“[d]</td><td colspan="5">see under
“Achievement of the radiological safety objectives“</td><td colspan="3"></td></tr>
</table>

[a] Prevention of mechanical interactions between fuel and cladding tube (Pellet Clad Interaction: PCI) which impair the unrestricted reuse of the fuel rods.
[b] For the approach to determine the design pressure of the containment see “Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation“ (Module 6), Annex 2.
[c] Criterion for ATWS events.
[d] under consideration of preceding radiological or technical requirements, if existing.

Table 3. 2: Safety-related acceptance targets and criteria of level of defence 2 to 4a for fuel element storage and handling

Level of defence:	**2**	**3**	**4a**
Operating phase:	**A – F**	**A – F**	**A – F**
Protection goal:	**Control of reactivity (R)**		
Acceptance target:	Ensuring subcriticality		
Acceptance criterion: neutron multiplication factor k_{eff}:	< 0.95	< 0.95 [a)]	< 0.99
Protection goal:	**Cooling of the fuel elements (K)** [c)]		
Acceptance targets:	Limitation of the pool water temperatures to values which ensure accessibility of the pool area with customary measures	Limitation of the pool water temperatures to values below the design temperature of the pool [b)]	Limitation of the pool water temperatures to values which ensure pool integrity [b)]
	Sufficient water coverage for ensuring the required inlet condition for the pool pumps	Sufficient water coverage for ensuring fuel element cooling	Sufficient water coverage for ensuring spill or evaporation cooling (maintenance of fuel rod integrity)
Protection goal:	**Confinement of radioactive material (B)** [c)]		
Acceptance targets:	See criteria for fuel element cooling		
Acceptance target:	Maintenance of the retention function of buildings and systems:		
Acceptance criteria:	see under “Achievement of the radiological safety objectives“[d)]	see under “Achievement of the radiological safety objectives“[d)]	-

[a] For special events (see event list Table 2.4): < 0.98.
[b] As far as accessibility of the containment or the pool area is required for maintenance of fuel element cooling, it is demonstrated that the conditions for accessibility are fulfilled.
[c] Acceptance targets only applicable to wet storage or handling processes.
[d] under consideration of preceding radiological or technical requirements, if existing.

Table 3.3: Radiological safety objectives of levels of defence 2 to 3 for the reactor plant and fuel element storage and handling

Level of defence:	2					3					4a
Operating phase:	**A**	**B**	**C**	**D**	**E**	**A**	**B**	**C**	**D**	**E**	**A – E**
	Achievement of the radiological safety objectives (S)										
Compliance with the specifications of the Radiation Protection Ordinance (StrlSchV):	Compliance with the limit values according to §§ 46, 47 StrlSchV					Compliance with the accident planning levels according to §49 StrlSchV					-

4 Definitions and classification of the operating phases for PWRs and BWRs

Table 4.1: Definition of the operating phases for PWRs and BWRs

Operating phase	Definition
A	Power operation via main heat sink. The operating phase covers all load conditions of the plant.
B	Startup of the plant or shutdown via main or auxiliary heat sink.
C	Residual-heat removal operation with the nuclear residual-heat removal system; primary system or reactor coolant system pressure-tight closed.
D	Residual-heat removal operation with the nuclear residual-heat removal system; primary system or reactor coolant system not pressure-tight closed; reactor cavity or reactor internals storage pool not or only partly flooded.
E	Residual-heat removal operation; reactor cavity or reactor internals storage pool completely flooded.
F	Fuel element cooling in fuel pool; core completely unloaded and fuel pool separated from reactor cavity or reactor internals storage pool.

Table 4.2: Operating phases during a standard inspection for refuelling in a PWR (starting with shutdown)

Operating phase	Start of operating phase	End of operating phase
A		Boron concentration has reached the value c(H-K) [a)] during plant shutdown.
B	Boron concentration ≥ c(H-K)[a)].	Heat removal exclusively via the secondary-side heat sink. Residual-heat removal cannot be performed via the primary-side heat sink (emergency core cooling and residual-heat removal system yet.
C	Residual-heat removal is performed via the primary-side heat sink (emergency core cooling and residual-heat removal system), primary circuit is pressure-tight closed.	The primary circuit is still pressure-tight closed.
D	The primary circuit is no longer pressure-tight closed.	The reactor cavity and the reactor internals storage pool have not been flooded completely yet.
E	The reactor cavity and the reactor internals storage pool are completely flooded.	The fuel elements are completely unloaded from the core, the refuelling slot gate has not been set yet.
F	The fuel elements are completely unloaded from the core, the refuelling slot gate has been set.	If core is completely unloaded into the fuel pool, the sealing function of the refuelling slot gate is no longer given.
	Reactor cavity and reactor internals storage pool are emptied for work on the primary circuit and then completely reflooded. In case of fuel shuffling in the core, operating phase F does not take place.	
E	Reactor cavity and reactor internals storage pool are completely flooded, sealing function of the refuelling slot gate is no longer given.	Reactor cavity and reactor internals storage pool are completely filled, draining is started.
D	Reactor cavity and reactor internals storage pool are no longer completely flooded.	Primary circuit is not yet pressure-tight closed.
C	The primary circuit is pressure-tight closed, residual heat is removed via the primary-side heat sink (emergency core cooling and residual-heat removal system).	Residual heat can still be removed via the primary-side heat sink (emergency core cooling and residual-heat removal system).
B	Residual heat cannot be removed via the primary-side heat sink (emergency core cooling and residual-heat removal system).	Boron concentration ≥ c(H-K).
A	Boron concentration <c(H-K).	

N o t e: In the above table, operating phases A-E occur twice, i. e. before and after refuelling.

[a)] Definition c(H-K): c(H-K) is the boron concentration at which at the respective burn-up condition of a xenon- and control-element-free cold core the shutdown reactivity required according to Table 3.1a for operating phase B is just ensured.

Table 4.3: Operating phases during standard inspection for refuelling in a BWR (starting with shutdown)

Operating phase	Start of operating phase	End of operating phase
A		Nuclear shutdown of the plant by insertion of the control rods; the control rods have not been inserted completely yet.
B	Nuclear shutdown of the plant was performed by complete insertion of the control rods.	Residual heat is only removed via the main heat sink. Residual heat cannot be removed via the primary-side heat sink (emergency core cooling and residual-heat removal system) yet.
C	Residual-heat removal is taken over by the nuclear residual-heat removal system or can be taken over by it, the reactor coolant system is pressure-tight closed.	The reactor coolant system is still pressure-tight closed.
D	The reactor coolant system is no longer pressure-tight closed.	The reactor cavity and the reactor internals storage pool have not been flooded completely yet.
E	The reactor cavity and the reactor internals storage pool have been flooded completely.	The reactor cavity and the reactor internals storage pool are still filled; draining is started.
D	The reactor cavity and the reactor internals storage pool are no longer completely flooded.	The reactor coolant system is not yet pressure-tight closed.
C	The reactor coolant system is pressure-tight closed; residual heat is removed via the nuclear residual-heat removal system or can be removed by it.	Residual-heat removal via the nuclear residual-heat removal system is ended for startup.
B	Residual-heat removal via the nuclear residual-heat removal system was ended for startup.	Withdrawal of the control rods is started for power generation; the control rods are still completely inserted.
A	Nuclear startup of the plant by withdrawal of the control rods; the control rods are no longer completely inserted.	
Special case for BWR		
F	The fuel elements are completely unloaded from the core, the refuelling slot gate has been set.	Withdrawal of the refuelling slot gate if core is completely unloaded into the fuel pool.
	For a BWR plant, operating phase F is only given in special cases (e.g. for RPV pressure test).	

N o t e: In the above table, operating phases A-D occur twice, i. e. before and after refuelling.

5 Event lists

N o t e: Explanations on the event lists

For low-power and shutdown operation of PWRs and BWRs as well as for the fuel pool, the event lists cover levels of defence 2 to 4a according to the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria” (Module 1). For level of defence 2, there is a comprehensive spectrum of events. For plant-specific analyses, this listing may be condensed to representative events, documented justification provided. For level of defence 3, representative events are listed for PWRs and BWRs. Moreover, the events to be considered for level of defence 4a are included. The approach on levels of defence 4b and 4c is presented in special regulations (see “Safety Criteria for Nuclear Power Plants: Criteria for Accident Management“ (Module 7)).

For the events listed in the following
- plant-internal fire with effects concerning more than one redundancy,
- plant-internal flooding,
- drop and impact of loads with potential risk for safety-relevant installations,
- drop of the fuel element transport cask,
- drop of heavy loads including fuel element transport cask onto the fuel pool,
- component failure with potential impact on safety-relevant installations,
- electromagnetic internal events,
- collision of vehicles at the plant site with safety-relevant systems, structures or components,
- plant-internal explosions, including radiolysis gas explosions in systems and components,
- extreme site-dependent events, such as ambient temperatures, flood, storm, snow, ice, lightning, external fire and, where applicable, other site-dependent events to be postulated, such as rock damage, ground settlement, mudslides, biological impacts in cooling water intakes (e.g. mussel growth, jellyfishes),
- impairment of heat removal by flotsam and ship accidents,
- electromagnetic external events,
- impacts of multi-unit plants or neighbouring plants,
- aircraft crash,
- plant-external explosion, plant-external fire, and
- intrusion of hazardous substances,

design criteria are specified in the “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components” (Module 10), Section 2 and 3, which ensure that consequences affecting more than one redundancy or other uncontrollable consequences cannot occur. Thus, no protection goals are assigned to the events in the event lists but reference is made to above-mentioned sections.

Events due to disruptive actions or other impacts by third parties are not subject of the event lists.

Within the different levels of defence, the event lists are divided into event categories.

The following event categories have been determined plant-type specifically for structuring of the lists. Here, it has to be considered that not all of the categories are of relevance at each plant operation condition or operating phase.

For PWRs, the event categories are:
- change of secondary-side heat removal,
- secondary-side heat removal - leakages,
- secondary-side heat removal - LOCAs,
- change of flow rate in the primary circuit,
- pressure change in the primary circuit,
- increase of reactor coolant inventory,
- decrease of reactor coolant inventory,
- loss of residual-heat removal,
- change of reactivity and power distribution,
- malfunction or leakage in nuclear auxiliary systems,
- loss of coolant within the containment,
- loss of coolant outside the containment,
- release of radioactive material from nuclear auxiliary systems,
- loss of energy supply,
- internal event,
- external event, and
- anticipated transient without scram (ATWS).

For BWRs:
- Main-steam- or feedwater-side change of heat removal,
- change of flow rate in the primary circuit,
- increase of reactor coolant inventory,
- decrease of reactor coolant inventory,
- loss of residual-heat removal,
- change of reactivity and power distribution,
- loss of coolant within the containment, not isolable
- loss of coolant outside the containment,
- malfunction or leakage in nuclear auxiliary systems,
- release of radioactive material from nuclear auxiliary systems,
- loss of energy supply,
- internal event,
- external event and
- anticipated transient without scram (ATWS).

For the fuel pool, the following event categories are applicable to both PWRs and BWRs:
- Reduced heat removal from the fuel pool,
- loss of coolant from the fuel pool,
- loss of energy supply,
- reactivity changes in the fuel pool,
- events during handling and storage of fuel elements and heavy loads,
- internal event, and
- external event.

The columns of the event lists begin with the numbering (Ey-x; y = level of defence and x represents the consecutive numbering of the events on the respective level) and the description of the events. This is followed by columns for the protection goals concerned, the relevant operating phases, additional comments on the acceptance criteria and, where appropriate, details on additional boundary conditions and event-specific notes.

The letters in the column “Protection goals concerned“ indicate for each event those protection goals for which effectiveness of the measures and systems is demonstrated. The acceptance criteria generally applicable to the different protection goals are –for both power operation (operating phase A) and low power and shutdown operation (operating phases B-F) of PWRs and BWRs as well as for the fuel pool – included in Table 3.1 which specifies the acceptance criteria for the levels of defence and operating phases.

Events for which there is the possibility to demonstrate effectiveness and reliability of preventive measures instead of demonstrating the effectiveness of measures and systems for the control of an event so that occurrence of these is so unlikely that it does not have to be postulated are referenced as VM.

The right column includes, where required, event-specific boundary conditions and detailed event-specific comments.

In the column “Operating phase“, those phases of nuclear power plant operation are presented in which the respective event may occur and may be of significance.

The lines of the lists begin with the indication of the level of defence. The following line indicates the event category from which the events listed in the following are derived.

For events with loss of coolant, a distinction is made between leakage and leak or break. A leakage is generally an event of level of defence 2. The leakage rate is so low that the safety system is not activated. Leaks or breaks, however, are exclusively events of level of defence 3. Here, the leakage rate is so high that the safety system is activated.

For leaks and breaks, the analysed maximum leak area depends on whether or not break preclusion is demonstrated for the pipe section considered. The specifications for the generally postulated leak cross sections and breaks are described in Annex 2.

Table 5.1: Event list for low-power and shutdown operation at PWRs

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
Level of defence 2					
Change of the secondary-side heat removal					
E2-01	Malfunction in the main steam system or in the feedwater supply system which leads to an unplanned temperature/pressure decrease in the steam generator or primary circuit	R	A		Note: E.g. control fault, loss of high-pressure feed heater, inadvertent actuation of a main steam turbine bypass, inadvertent actuation of auxiliary steam supply.
E2-02	Malfunction in the main steam system or in the feedwater supply system which leads to an unplanned temperature/pressure increase in the steam generator or primary circuit	K	A-B		Note: E.g. turbine control faults, partially inadvertent closure of main steam isolation valves.
E2-03	Inadvertent closure of valves leading to significant changes in main steam or feedwater flow rate.	K B	A-B		
E2-04	Turbine trip with opening of the turbine bypass or delayed loss of the bypass station	R K B	A		
E2-05	Turbine trip without opening of the turbine bypass	R K B	A		
E2-06	Loss of main heat sink	R K B S	A-B		Additional boundary condition: Operationally permissible steam generator tube leakages are considered.
E2-07	Load rejection to auxiliary power	R K B	A		Additional boundary condition: With and without switching to off-site power supply.
E2-08	Loss of some main feedwater pumps	R K	A		

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
Secondary-side heat removal - leakages					
E2-09	Leakage in main steam or feedwater system including steam generator blowdown system within the containment	B	A-B		N o t e: No challenge of the reactor protection criterion "differential pressure between equipment/service compartments and atmosphere: ΔpComp-Atm > 30 hPa".
E2-10	Main steam or feedwater leakage outside the reactor building (after first isolation valve or anchor point)	B S	A-B		A d d i t i o n a l b o u n d a r y c o n d i t i o n: Operationally permissible steam generator tube leakages are considered.
Change of flow rate in the primary circuit					
E2-11	Loss of a main coolant pump	R K	A-B		
E2-12	Loss of all main coolant pumps	R K B	A-B		
E2-13	Break of a main coolant pump shaft	R K	A		A d d i t i o n a l b o u n d a r y c o n d i t i o n: Immediate blocking of the impeller is also considered.
Pressure change in the primary circuit					
E2-14	Pressure drop due to inadvertent pressuriser spraying actuation or inadvertent valve opening	K	A-B		
E2-15	Pressure increase due to inadvertent switch-on of pressuriser heater	B	A-C		

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
Increase of reactor coolant inventory					
E2-16	Inadvertent injection or reduction of extraction rates by operational systems or safety systems	K B	A-C		
Decrease of reactor coolant inventory					
E2-17	Inadvertent opening of a pressuriser safety valve or pressuriser relief valve for a short time	K B	A-C		Additional boundary condition: – For a short time so that the rupture discs of the pressuriser relief tank remain intact. – For the pressuriser safety valve, only operating phases B and C are considered.
E2-18	Leakages from steam generator tubes	S	A-C		Note: Event serves to determine the maximum permissible activity concentration in the secondary circuit in case of steam generator tube leakages.
E2-19	Malfunction in the volume control system leading to a reduction of the coolant inventory	K	A-C		
E2-20	Level drop during mid-loop operation	K B	C-D		
E2-21	Leakages from primary circuit and connecting pipes	B S	A-E		
E2-22	Leakages from coolers carrying primary coolant	B S	A-E		
Loss of residual-heat removal					
E2-23	Loss of a train, in operation or in demand, of the residual-heat removal system including cooling chain	K B	C-E		Additional boundary condition: Single failure is not postulated
E2-24	Loss of all residual-heat removal trains due to faulty reactor protection signals	K B	C-E		

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
Change of reactivity and power distribution					
E2-25	Malfunction in the reactor power control system	R K	A		
E2-26	Maximum reactivity insertion due to withdrawal of single control elements or control element groups	R K	A		
E2-27	Inadvertent drop or insertion of one or more control elements	R K	A		
E2-28	Inadvertent injection from a system carrying unborated water or low-borated coolant (external boron dilution; homogeneous and heterogeneous)	R	A-E		
E2-29	Most unfavourable misloading of a most reactive fuel element	R K	E, A	Protection goal R (subcriticality) in operating phase E Protection goal K in operating phase A	Additional boundary condition: Reactor startup with misloaded fuel element is analysed regarding protection goal K in operating phase A.
E2-30	Non-compliance with the switch-on conditions when switching on a main coolant pump	R K	A		
E2-31	Cold water injection into the reactor coolant system from a connected system (e.g. bypass of the recuperative heat exchanger of the volume control system)	R	A-B		
Malfunction or leakage in nuclear auxiliary systems					
E2-32	Malfunction or leakage in off-gas and waste water treatment system or in other nuclear auxiliary systems with radiological consequences	S	A-F		
E2-33	Inadvertent flushing or evacuation operation	S	C		
Loss of energy supply					
E2-34	Loss of offsite power for less than 2 hours	R K B	A-E		Additional boundary condition: Operationally permissible steam generator

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
		S			tube leakages are considered.
Internal event					
E2-35	Loss of ventilation/cooling	- - -	A-E	Specification of the acceptance targets: Safe confinement of activities in the controlled area (subatmospheric pressure system). Compliance with specified ambient conditions for electrical and I&C components.	Additional boundary condition: For ventilation/cooling systems, compliance with specified ambient conditions for electrical and I&C components and their operability is demonstrated. For the controlled area, compliance with the conditions for the system functions (temperature max/min) and the radiological monitoring functions (e.g. pressure differences) is demonstrated in addition.

Level of defence 3					
Change of the secondary-side heat removal					
E3-01	Major malfunction in the main steam system or in the feedwater supply system, leading to an unplanned temperature or pressure reduction in the steam generator or in the primary circuit	R B S	A-C		Additional boundary condition: Operationally permissible steam generator tube defects are considered. Note: E.g. inadvertent complete opening of main steam bypass valve, inadvertent opening of main steam safety and main steam relief valves. Relevant with regard to radiology (since no N16 detection) in phase B or in phase A at low power. Inadvertent opening in phase B more probable than in phase A due to performance of tests.
E3-02	Major malfunction in the main steam system or in the feedwater supply system, leading to an unplanned temperature or pressure reduction in the steam generator or in the primary circuit	K B	A-B		Additional boundary condition: Cases considered: e.g. two up to all main steam isolation valves.
E3-03	Loss of feedwater supply	K	A-B		

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E3-04	Malfunction in the feedwater supply, leading to an impermissible increase of the coolant level in the steam generator or flooding of the main steam line	K	A-B		
Secondary-side heat removal – leaks					
E3-05	Secondary-side leak or secondary-side break within the containment	R K B	A-C		Additional boundary condition: – Details on the leak or break assumptions and on safety demonstrations are included in Annex 2. – At low secondary circuit pressures, the effectiveness of the actuation due to dp/dt and / or containment pressure difference at the respective leak spectrum has to be considered.
E3-06	Leak/break in main steam or feedwater system or other high-energy piping systems in the annulus and in the valve compartment	R K B S VM	A-B	Criteria for potential preventive measures: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components” (Module 10)	Additional boundary condition: – Operationally permissible steam generator tube defects are considered for leak/break in the main steam and feedwater system. – Details on the leak or break assumptions and on safety demonstrations are included in Annex 2. Special consideration of: – the integrity of the containment, – humidity, pressure build-up, differential pressures, temperature, jet and reaction forces, etc. with impacts affecting more than one redundancy, and – the integrity of safety-relevant structures of the reactor building and the valve compartment.
E3-07	Leak/break in main steam or feedwater system outside the containment building (up to and including first isolation valve and anchor point)	R K B	A-C		Additional boundary condition: Operationally permissible steam generator tube defects are considered for leak/break of

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
		S			the main steam line. Details on the leak or break assumptions and on safety demonstrations are included in Annex 2.
E3-08	Main steam line rupture after first isolation with maximum 2A break of a steam generator tube	R K B S	A-B		Additional boundary condition: Details on the leak or break assumptions and on safety demonstrations are included in Annex 2.
E3-09	Inadvertent opening of a main steam safety valve with consequential 2A break of a steam generator tube	R K B S	A-B		
Increase of reactor coolant inventory					
E3-10	Inadvertent injection by operational systems or safety systems in case of ineffectiveness of limitation measures provided	K B	A-C		
Decrease of reactor coolant inventory					
E3-11	Inadvertent level drop during mid-loop operation with consequential loss of residual-heat removal pumps	R K B	C-D	Protection goal R affected due to reflux condenser mode in Phase C. Protection goal B is relevant for operating phase C (primary circuit closed)	
Loss of residual-heat removal					
E3-12	Loss of a train, in operation or in demand, of the residual heat-removal system including cooling chain	K B	C-E		Additional boundary condition: In contrast to event E2-23, here with consideration of the single failure according to “Safety Criteria for Nuclear Power Plants:

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
					Criteria for the Design and Safe Operation of Plant Structures, Systems and Components" (Module 10).
Change of reactivity and power distribution					
E3-13	Inadvertent withdrawal of the most effective control element or control element group with loss of limitation systems	R K	A		
E3-14	Ejection of the most effective control element	R K	A		Note: See also "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Operation of the Reactor Core" (Module 2), subsection 6.3 (6).
E3-15	Misloading of the reactor core with more than one fuel element	R VM	E	Criteria for potential preventive measures: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components", Section 4.2.3 (Module 10).	
E3-16	Drop of a fuel element on the reactor core	R	E		Additional boundary condition: Verification of subcriticality for fuel element on the core
E3-17	Inadvertent injection from a system carrying unborated water or low-borated coolant with loss of limitation systems or preceding procedures (external boron dilution; homogeneous and heterogeneous)	R K VM	A-E	Criteria for potential preventive measures: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components",	Additional boundary condition: The following is considered: - Inadvertent filling of tanks, - input from connected systems via heat exchanger tubes, seals and / or valve seat leakages, and - inadvertent injection into the primary

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
				Section 4.2.1(Module 10).	circuit. - feedwater injection during shutdown under loss of offsite power conditions after steam generator tube rupture. It is demonstrated that reactivity changes due to injection of unborated water into the reactor coolant system remains limited to such values where - for an initially critical reactor the safety-related acceptance target for the reactivity accident according to Table 3.1b and - for an initially subcritical reactor the amount of shutdown reactivity required according to Table 3.1a are complied with.
E3-18	Formation of low-borated areas in the primary circuit (internal boron dilution)	R K VM	A-C	Criteria for potential preventive measures: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components” (Module 10).	Additional boundary condition: Potential sources of formation of low-borated areas are investigated. Causes may be, e.g., - reflux condenser operation after small LOCA under consideration of the inserted control elements (under consideration of Module 1, subsection 3.2 (6)) and the time-dependent xenon concentration, and - shutdown with three circuits and secondary-side isolated steam generator and injection of low-borated coolant after restart of natural circulation. - VM only for the prevention of additional switch-on of main coolant pumps during or after reflux condenser operation. - It is demonstrated that reactivity changes due to injection of unborated water into the reactor coolant system remains

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
					limited to such values where for an initially subcritical reactor the amount of shutdown reactivity required according to Table 3.1a is complied with.
E3-19	Subcooling transients due to leak or break of main steam or feedwater line	R K	A	Specification of the acceptance criteria: Recriticality permissible for leaks in main steam line ≥ 0.1 A, inasmuch as the criteria for cooling of the fuel elements are fulfilled.	
Loss of coolant within the containment					
E3-20	Small leak within the containment	R K B S	A-B		Additional boundary condition: - Reflux condenser mode is considered (see E3-21). - Details on the leak or break assumptions and on safety demonstrations are included in Annex 2. - Safety demonstrations also comprise “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.8.3 (Module 10). Note: Characteristic feature: Secondary-side heat removal necessary for the control of that design basis accident.
E3-21	Medium leak within the containment (leak cross section ≤ 0.1 A)	R K B S	A-B		Additional boundary condition: - For details on the leak or break assumptions and on the required safety demonstrations, see Annex 2. - Safety demonstrations also comprise

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
					“Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.8.3 (Module 10). Note: Characteristic feature of the medium leak: Heat removal via leak sufficient => secondary-side heat removal for control of that design basis accident not generally necessary.
E3-22	Large leak within the containment (leak cross section > 0.1 A)	R K B S	A-B	Specification of the acceptance criteria: Subcriticality in the short term without taking the control elements into account unless effectiveness of the control elements has not been demonstrated, and in the long term without taking the control elements into account..	Additional boundary condition: - Details on the leak or break assumptions and on safety demonstrations are included in Annex 2. - The double-ended break of a main coolant line (“2A break“) determines the dimensioning of the emergency core cooling and residual-heat removal system, the pressure design of the containment, the design of the pump flywheels against failure due to overspeed and the failure resistance of all safety-relevant components in the containment required for the control of accidents. - Safety demonstrations also comprise “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.8.3 (Module 10).
E3-23	Leak at the connecting nozzle of the main coolant line on reactor pressure vessel	K	A-B		Additional boundary condition: - It is demonstrated that impermissible impacts on the structure of the reactor

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
					cavity and the anchoring of the reactor pressure vessel are excluded. Further, the consequences of an event regarding sufficient coverage of sump suction lines with coolant in case of considered dead volumes of the reactor cavity are considered.
E3-24	“20 cm^2“ leak in reactor pressure vessel below upper edge of the core	R K B S	A-B		Additional boundary condition: The leak size of 20 cm² is design-relevant for the flow-off conditions at the biological shield and the maintenance of its safety function.
E3-25	Leak in RPV closure head area	R K B S	A-B		Additional boundary condition: - For the control of events it is demonstrated in particular that sufficient drainage of the coolant into the containment sump is also ensured under consideration of the routine operating processes and after plant shutdown. - Details on the leak or break assumptions and on safety demonstrations are included in Annex 2.
E3-26	Leak due to faulty maintenance or switching failures at the primary circuit	K B S	C-E		Additional boundary condition: - The leak size is determined by the largest free cross section in the lines connected with the primary circuit or its components (e.g. manholes). - The analysis considers that in case of an incident a fuel element is transported in the most unfavourable position. Here, the acceptance criterion is maintenance of cladding tube integrity. - Requirement for emergency cooling effectiveness; limited availability of safety installation (e.g. reactor protection) is considered.

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E3-27	Inadvertent opening and / or stuck-open of a pressuriser safety valve or pressuriser relief valve, e.g. during functional tests	K B	B-C		Additional boundary condition: The limited availability of safety installation (e.g. reactor protection) is considered.
E3-28	Failure of a steam generator tube (larger than operationally permissible leakages and up to max. 2A)	K B S	A-B		Additional boundary condition: The event is investigated with and without reaching the limit value of the main steam activity regarding actuation of the reactor protection system. Without actuation, e.g. at small thermal load, zero load or 3- or 2-loop operation.
Loss of coolant outside the containment					
E3-29	Leak in residual-heat removal system in annulus during residual-heat removal operation	K B S	C-E		Additional boundary condition: Spiking effect is considered.
E3-30	Leak/break in heat exchangers carrying primary coolant in case of demand	K B S	A-E		Additional boundary condition: Leak size: up to 2A of an exchanger tube.
E3-31	Loss of coolant from the containment via systems connected to the reactor coolant pressure boundary	K B S	A-C		
E3-32	Leaks in systems with flooding potential in the annulus	R K B S	A-E		Additional boundary condition: - All relevant sources from leaks and containment failure of systems and devices in the annulus, in particular the containment sump suction line, are considered. - Further, the boundary conditions within the framework of maintenance measures are considered (see also “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.2 (Module 10).

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
Release of radioactive material from nuclear auxiliary systems					
E3-33	Leak in the volume control system outside the containment	S	A-F		Additional boundary condition: - Details on the leak or break assumptions and on safety demonstrations are included in Annex 2. - Spiking effect is considered.
E3-34	Leak in an instrumentation line, carrying primary coolant, in the annulus	S	A-F		Additional boundary condition: Spiking effect is considered.
E3-35	Leak/break in a pipe or break of a filter in the off-gas or gas treatment system	S	A-F		
E3-36	Leak in container with active medium	S	A-F		Additional boundary condition: The container with the largest radiological hazard potential is identified.
Loss of energy supply					
E3-37	Loss of offsite power for more than 2 hours	R K S	A-E		Additional boundary condition: Operationally permissible steam generator tube leakages are considered.
Internal event					
E3-38	Plant-internal fire with impacts affecting more than one redundancy	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.1 (Module 10).
E3-39	Plant-internal fire including filter fire and explosion	S	A-F		Additional boundary condition: Performance of analyses on fires and explosions at components or system areas with high activity release potential.

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E3-40	Plant-internal flooding	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.2 (Module 10).
E3-41	Drop and impact of loads with potential risk for safety-relevant installations	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.4 (Module 10).
E3-42	Break of a control element nozzle or control element ejection	R K B S	A-B		Additional boundary condition: In addition to the control of the resulting leak it is demonstrated that the ejection of the control element does not lead to an impermissible damage of the containment. Further, it is demonstrated that no consequential damages of neighbouring drives occur that impair the functional safety of other control elements. If consequential damage cannot be excluded, it is demonstrated that the acceptance criteria are also fulfilled.
E3-43	Component failure with potential impact on safety-relevant installations	Design requirement	A-F		Additional boundary condition: - Details on the leak or break assumptions and on safety demonstrations are included in Annex 2. See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.3 (Module 10).

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E3-44	Electromagnetic internal events (except lightning)	Design requirement	A-F		Additional boundary condition: - See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.5 (Module 10).
E3-45	Collision of vehicles at the plant site with safety-relevant, structures or components	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.6 (Module 10).
E3-46	Plant-internal explosions, including radiolysis gas explosions in systems and components	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.8 (Module 10).
External event					
E3-47	Earthquake (including consequential impacts)	S Design requirement	A-F		Additional boundary condition: - Postulation of failure of that container which represents all others radiologically. - See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 3.2.3.2 (Module 10).

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E3-48	Extreme site-dependent events, such as ambient temperatures, flood, storm, snow, ice, lightning, external fire and, where applicable, other site-dependent events to be postulated, such as rock damage, ground settlement, mudslides, biological impacts in cooling water intakes (e.g. mussel growth, jellyfishes)	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 3.2.3 (Module 10).
E3-49	Impairment of heat removal by flotsam and ship accidents	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 3.2.2.1 (Module 10).
E3-50	Electromagnetic external events (except lightning)	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 3.2.2.2 (Module 10).
Level of defence 4					
Level of defence 4a					
Anticipated transient without scram (ATWS)					
E4a-01	Loss of main heat sink, e.g. by loss of condenser vacuum or closure of the main steam isolation valve with available auxiliary power supply	R K B	A		
E4a-02	Loss of main heat sink with unavailable auxiliary power supply	R K B	A		
E4a-03	Maximum increase of steam extraction, e.g. by opening of the bypass station or of the main steam safety valves	R K B	A		
E4a-04	Total loss of main feedwater supply	R K B	A		

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E4a-05	Maximum reduction of the coolant flow rate	R K B	A		
E4a-06	Maximum reactivity insertion by withdrawal of control elements or control element groups on the basis of the operating conditions “full load” and “hot subcritical”	R K B	A		
E4a-07	Depressurisation due to inadvertent opening of a pressuriser safety valve	R K B	A		
E4a-08	Maximum reduction of the reactor inlet temperature caused by a fault in an active component of the feedwater supply	R K B	A		
External event					
E4a-09	Functional failure of the control room	R K B	A-F		
E4a-10	Impacts of multi-unit plants or neighbouring plants	Design requirements	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.7 (Module 10).
E4a-11	Aircraft crash	Design requirements	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 3.2.1.1 (Module 10).

No.	PWR events	Protection goals concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E4a-12	Plant-external explosion, plant-external fire	Design requirements	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 3.2.1.2 and 3.2.1.3 (Module 10).
E4a-13	Intrusion of hazardous substances	Design requirements	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 3.2.1.4 (Module 10).

Table 5.2: Event list for low-power and shutdown operation in BWRs

No.	BWR events	Protection goal concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
Level of defence 2					
Main-steam- or feedwater-side change of heat removal					
E2-01	Malfunctions in the main steam system or in the feedwater supply system which lead to an unplanned temperature or pressure decrease in the reactor coolant system	K	A-B		Additional boundary condition: Impact on stability of the core is considered. Note: E.g. control fault, loss of high-pressure preheater, inadvertent actuation of a main steam turbine bypass, inadvertent actuation of auxiliary steam supply.
E2-02	Malfunctions in the main steam system or in the feedwater supply system which lead to an unplanned temperature/pressure increase in the reactor coolant system	R K	A-B		Note: - E.g. malfunction of turbine control, inadvertent closure of individual valves. - Challenge of the pressure control, in particular of the main steam bypass.
E2-03	Turbine trip with opening of the turbine bypass or with delayed loss of the bypass	R K B	A		
E2-04	Turbine trip without opening of the turbine bypass station	R K B	A		
E2-05	Loss of main heat sink	R K B	A-B		
E2-06	Load rejection to auxiliary power	R K B	A		Additional boundary condition: With and without switch over to offsite power.
E2-07	Loss of a main feedwater pump	R K	A-B		

No.	BWR events	Protection goal concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E2-08	Loss of all main feedwater pumps	R K	A-B		
			Change of flow rate in the primary circuit		
E2-09	Loss of individual / several / all reactor recirculation pumps	R K	A-B		Additional boundary condition: Impact on stability of the core is considered.
			Increase of reactor coolant inventory		
E2-10	Malfunction in the coolant level control or removal of excess water or inadvertent injection by operational systems or safety systems	R B	A-C		Note: Relevant for level limitation. Prevention of water entry into the main steam line.
E2-11	Inadvertent injection with a train of the emergency core cooling systems	- - -	D	Specification of the acceptance criteria: Ensuring coolant inventory in the long term	Additional boundary condition: - Relevant for procedures. - Only relevant in operating phase D due to overfilling of reactor pressure vessel in case of not installed reactor cavity seal liner.
			Decrease of reactor coolant inventory		
E2-12	Leakage from the main steam or feedwater system within the containment	S	A-B		
E2-13	Leakage from the main steam or feedwater system within the reactor building	S	A-B		
E2-14	Leakage from the main steam or feedwater system within the turbine hall	S	A-B		
E2-15	Leakage from coolers carrying reactor coolant	S	A-E		Note: Relevant for monitoring.
E2-16	Leakage from connecting pipes of the reactor coolant system within the containment	- - -	A-C	Specification of the acceptance criteria: Leakage detection	Note: Relevant for monitoring.

No.	BWR events	Protection goal concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E2-17	Leakage from RPV bottom resulting from maintenance work	K	E		Note: - Relevant for procedures. - Limit: leakage can be overfed by operational systems.
	Loss of residual-heat removal				
E2-18	Loss of a train, in operation or in demand, of the residual-heat removal system including cooling chain	K B	C-E		Additional boundary condition: Single failure is not postulated
E2-19	Shutdown of all residual-heat removal trains due to pressure increase or coolant level decrease	K B	C-E		
	Change of reactivity and power distribution				
E2-20	Maximum reactivity insertion due to withdrawal of single control rods or control rod groups	R K	A		
E2-21	Inadvertent fast rod insertion or inadvertent insertion of a control rod	K	A		
E2-22	Inadvertent insertion of all control rods at high power	R B	A		
E2-23	Maximum reduction of the reactor inlet temperature caused by a fault in an active component of the feedwater supply or by inadvertent injection by operational systems or safety systems (subcooling transient)	R K	A		Additional boundary condition: Impact on stability of the core is considered.
E2-24	Malfunction in the reactor power control	R K	A		
E2-25	Most unfavourable misloading of a most reactive fuel element	R K	E, A	Protection goal R (subcriticality) in operating phase E Protection goal K in operating phase A	Additional boundary condition: Reactor startup with misloaded fuel element is analysed regarding protection goal K in operating phase A.

No.	BWR events	Protection goal concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E2-26	Inadvertent speed increase of the reactor recirculation pumps	R K	A-B		Additional boundary condition: Increase of pump speed from minimum speed with maximum speed gradient.
Malfunction or leakage in nuclear auxiliary systems					
E2-27	Malfunction or leakage in off-gas and waste water treatment system or in other nuclear auxiliary systems with radiological consequences	S	A-F		
E2-28	Inadvertent flushing or evacuation operation	S	C		
Loss of energy supply					
E2-29	Loss of offsite power for less than 2 hours	R K B S	A-E		
Internal event					
E2-30	Loss of ventilation / cooling	- - -	A-E	Specification of the acceptance criteria: Safe confinement of activities in the controlled area (subatmospheric pressure system). Compliance with specified ambient conditions for electrical and I&C components.	Additional boundary condition: - For ventilation/cooling systems, compliance with specified ambient conditions for electrical and I&C components and their operability is demonstrated. - For the controlled area, compliance with the conditions for the system functions (temperature max/min) and the radiological monitoring functions (e.g. pressure differences) is demonstrated in addition.
Level of defence 3					
Main-steam- or feedwater-side change of the removal					

No.	BWR events	Protection goal concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E3-01	Major malfunction in the main steam system or in the feedwater supply system which leads to an unplanned temperature or pressure decrease in the reactor coolant system.	R K	A-B		N o t e: E.g. inadvertent complete opening of main steam bypass valve, inadvertent opening of main steam safety and main steam relief valves.
E3-02	Major malfunction in the main steam system or in the feedwater supply system which leads to an unplanned temperature or pressure increase in the reactor coolant system.	R K B	A-B		N o t e: E.g. inadvertent closure of all main steam isolation valves.
E3-03	Loss of a high-pressure injection train after loss of the main feedwater pumps	R K	A		
Increase of reactor coolant inventory					
E3-04	Functional failure with increase of coolant level in the reactor pressure vessel or inadvertent injection by operational systems of safety systems and unavailability of limitation systems	R B	A-C		
Decrease of reactor coolant inventory					
E3-05	Inadvertent level drop in the reactor pressure vessel with consequential switch-off of the residual-heat removal pumps	K	C-D		
Loss of residual-heat removal					
E3-06	Loss of a train, in operation or in demand, of the residual-heat removal system including cooling chain	K B	C-E		A d d i t i o n a l b o u n d a r y c o n d i t i o n: In contrast to event E2-19, here with consideration of the single fault according to “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components” (Module 10).
Change of reactivity and power distribution					
E3-07	Inadvertent reactivity insertion due to loss of	R	A		

No.	BWR events	Protection goal concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
	high-pressure preheater and unavailability of limitation systems	K			
E3-08	Withdrawal of the most effective control element or control element group with loss of limitation systems	R K	A		
E3-09	Ejection of the most effective control rod	R K	A		Note: Also see "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Operation of the Reactor Core" (Module 2), subsection 6.3 (6).
E3-10	Drop out of the most effective control rod	R K	A		Additional boundary condition: Drop out over the length of a latch distance.
E3-11	Drop of a fuel element into the just not yet critical reactor core	R K VM	E	Criteria for potential preventive measures: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components", Section 4.2.2 (Module 10).	
E3-12	Drop of a fuel element onto the reactor core	R	E		Additional boundary condition: Verification of subcriticality for fuel element on the core.

No.	BWR events	Protection goal concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E3-13	Inadvertent withdrawal of control rods during loading	R K VM	E	Criteria for potential preventive measures: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components", Section 4.2.2 (Module 10).	
E3-14	Inadvertent withdrawal of a control rod during shutdown safety test	R K	E		
E3-15	Misloading of the reactor core with more than one fuel element	R VM	E	Criteria for potential preventive measures: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components", Section 4.2.3 (Module 10).	
E3-16	Nuclear-thermal hydraulic instability	R K	A		Additional boundary condition: - In-phase and out-of-phase oscillations are analysed. - The boundary conditions of the potential initiating events are considered.

No.	BWR events	Protection goal concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E3-17	Inadvertent speed increase of the reactor recirculation pumps	R K	A		Additional boundary condition: Increase of pump speed from minimum speed with maximum speed gradient without consideration of limitation systems.
Loss of coolant within the containment, not isolable					
E3-18	Leak/break within the containment (leak cross section ≤ 0.1 A of the main steam line)	R K B S	A-B		Additional boundary condition: - In-addition to main steam and feedwater lines, all other coolant-retaining systems are considered. - Details on the leak or break assumptions and on safety demonstrations are included in Annex 2. - Safety demonstrations also comprise “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.8.3 (Module 10).
E3-19	Leak/break within the containment (leak cross section ≤ 0.1 A of the main steam line)	R K B S	A-B		Additional boundary condition: - Details on the leak or break assumptions and on safety demonstrations are included in Annex 2. - The double-ended break of a main steam line (“2A break“) determines the dimensioning of the pressure suppression system, of the RPV internals required for shutdown and core cooling, of the emergency core cooling and residual-heat removal system as well as the pressure design of the containment and the failure resistance of all safety-relevant systems and components required for the control

No.	BWR events	Protection goal concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
					of events. - Safety demonstrations also comprise “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.8.3 (Module 10). .
E3-20	“80 cm^2“ leak in RPV bottom	R K B S	A-B		
E3-21	Leak due to faulty maintenance or switching failures at the reactor coolant system	K	C-E		Additional boundary condition: - A maximum leak resulting from faulty maintenance or switching failures is postulated. The leak size is determined by the largest free cross section in the lines connected with the reactor coolant system - The analysis considers that in case of an incident a fuel element is transported in the most unfavourable position. Here, the acceptance criterion is the integrity of the cladding tube. Note: This may result in requirements for the sump function of the containment (locks included).
E3-22	Leak in the reactor cavity seal liner	K S	D-E		Additional boundary condition: - The constructively possible leak cross section in case of seal failure is postulated. - Relevant for establishment of the sump

No.	BWR events	Protection goal concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
					function and procedures.
E3-23	Leak in RPV bottom due to - inadvertent pulling of a pump shaft, or - work on control rod drives or detector assemblies	K S	E		Note: Where applicable, temporary requirement for the sump function of the containment until reliable function of the isolating equipment has been verified (locks included).
E3-24	Loss of tightness between drywell and wetwell	R K B S VM	A-B	Criteria for potential preventive measures: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 4.2.5 (Module 10).	
Loss of coolant outside the containment					
E3-25	Leak/break in the main steam or feedwater system and other high-energy piping systems between containment and first isolation possibility outside the containment	R K B S VM	A-B	Criteria for potential preventive measures: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 4.2.4 (Module 10).	Additional boundary condition: - Details on the leak or break assumptions and on safety demonstrations are included in Annex 2. Special consideration of: – the integrity of the containment, – humidity, pressure build-up, differential pressures, temperature, jet and reaction forces, etc. with impacts affecting more than one redundancy, and – the integrity of safety-relevant structures of the reactor building.
E3-26	Leak/break in the main steam or feedwater system within the turbine building	R K	A-B		Additional boundary condition:

No.	BWR events	Protection goal concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
		B S			For details on the leak or break assumptions and on the required safety demonstrations, see Annex 2.
E3-27	Leak/break in an instrumentation line carrying coolant, in the reactor building	S	A-C		Additional boundary condition: – 2A break of an instrumentation line in the reactor building that cannot be isolated for 30 min. – The most unfavourable operating phase is analysed with regard to radiology (spiking effect).
E3-28	Leak/break in the reactor water cleanup system in the reactor building	S	A-E		Additional boundary condition: Spiking effect is considered.
E3-29	Leak/break in coolers, carrying reactor coolant, in case of demand	B S	A-E		
E3-30	Leakage from the wetwell	K B	A-B		Additional boundary condition: - Details on the leak or break assumptions and on safety demonstrations are included in Annex 2. - The event is relevant for the transition to residual-heat removal via RHR train from RPV and flooding of reactor building.
E3-31	Leak in pressure relief pipe of the wetwell	K B S	A-B		
E3-32	Leak/break in reactor scram system in the reactor building	R B	A		Note: Relevant for the design of the reactor scram system.
E3-33	Leak in residual-heat removal system in the reactor building during residual-heat	K B	C-E		Additional boundary condition:

No.	BWR events	Protection goal concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
	removal operation	S			Spiking effect is considered.
E3-34	Loss of coolant from the containment via systems connected to the reactor coolant pressure boundary	B S	A-C		
Release of radioactive material from nuclear auxiliary systems					
E3-35	Leak/break in a pipe or break of a filter in the off-gas or gas treatment system	S	A-F		
E3-36	Leak in container with active medium	S	A-F		N o t e: The container with the largest radiological hazard potential is identified.
Loss of energy supply					
E3-37	Loss of offsite power for more than 2 hours	R K S	A-E		
Internal event					
E3-38	Plant-internal fire and / or plant-internal explosion with impacts affecting more than one redundancy	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.1 (Module 10).
E3-39	Plant-internal fire including filter fire and explosion	S	A-F		Additional boundary condition: Performance of analyses on fires and explosions affecting components or system areas with high activity release potential.

No.	BWR events	Protection goal concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E3-40	Plant-internal flooding	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.2 (Module 10).
E3-41	Drop and impact of loads with potential risk for safety-relevant installations	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.4 (Module 10).
E3-42	Break of a control rod nozzle or control rod ejection	R K B S	A-B		Additional boundary condition: In addition to the control of the resulting leak it is demonstrated that the ejection of the control rod does not lead to an impermissible damage of the containment. Further, it is demonstrated that no consequential damages of neighbouring drives occur that impair the functional safety of other control rods. If consequential damage cannot be excluded, it is demonstrated that the acceptance criteria are also fulfilled.
E3-43	Component failure with potential impact on safety-relevant installations	Design requirement	A-F		Additional boundary condition: - Details on the leak or break assumptions and on safety demonstrations are included in Annex 2. - See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.3 (Module 10).

No.	BWR events	Protection goal concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E3-44	Electromagnetic internal events (except lightning)	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.5 (Module 10).
E3-45	Collision of vehicles at the plant site with safety-relevant, structures or components	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.6 (Module 10).
E3-46	Plant-internal explosions, including radiolysis gas explosions in systems and components	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.8 (Module 10).
External event					

No.	BWR events	Protection goal concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E3-47	Earthquake (including consequential impacts)	S Design requirement	A-F		Additional boundary condition: - Postulation of failure of that container which represents all others radiologically. See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 3.2.3.2 (Module 10).
E3-48	Extreme site-dependent events, such as ambient temperatures, flood, storm, snow, ice, lightning, external fire and, where applicable, other site-dependent events to be postulated, such as rock damage, ground settlement, mudslides, biological impacts in cooling water intakes (e.g. mussel growth, jellyfishes)	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 3.2.3 (Module 10).
E3-49	Impairment of heat removal by flotsam and ship accidents	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 3.2.2.1 (Module 10).
E3-50	Electromagnetic external events (except lightning)	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 3.2.2.2 (Module 10).
Level of defence 4					
Level of defence 4a					
Anticipated transient without scram (ATWS)					

No.	BWR events	Protection goal concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E4a-01	Loss of main heat sink, e.g. by loss of condenser vacuum or closure of the main steam bypass valve with available auxiliary power supply	R K B	A		N o t e: For ATWS it is postulated that the nut backlash for the control rods is effective.
E4a-02	Loss of main heat sink with unavailable auxiliary power supply	R K B	A		
E4a-03	Maximum increase of steam extraction, e.g. by opening of the bypass station or of the safety and relief valves	R K B	A		
E4a-04	Total loss of main feedwater supply	R K B	A		
E4a-05	Maximum reactivity insertion by withdrawal of control rods or control element rods on the basis of the operating conditions "full load" and "hot zero power condition"	R K B	A		
E4a-06	Maximum decrease of the feedwater temperature	R K B	A		
E4a-07	Steam line isolation with available auxiliary power supply	R K B	A		
E4a-08	Steam line isolation with unavailable auxiliary power supply	R K B	A		
E4a-09	Maximum increase of feedwater flow rate	R K B	A		

No.	BWR events	Protection goal concerned	Opera-ting phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
E4a-10	Startup of the recirculation pumps with maximum speed gradient	R K B	A		
External event					
E4a-11	Functional failure of the control room	R K B	A-F		
E4a-12	Impacts of multi-unit plants or neighbouring plants	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.7 (Module 10).
E4a-13	Aircraft crash	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 3.2.1.1 (Module 10).
E4a-14	Plant-external explosion, plant-internal fire	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 3.2.1.2 and 3.2.1.3 (Module 10).
E4a-15	Intrusion of hazardous substances	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 3.2.1.4 (Module 10).

Table 5.3: Event list fuel pool PWR and BWR

No.	Fuel element handling and storage events for PWRs and BWRs	Protection goals concerned	Opera-tional phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
Level of defence 2					
Reduced heat removal from the fuel pool					
E2-01	Loss of a train in operation or unplanned short-term (max. 30 min) interruption of heat removal	K	A-F		
Loss of coolant from fuel pool					
E2-02	Leakage from the fuel pool or its cooling and purification systems	K	A-F		
Loss of energy supply					
E2-03	Loss of offsite power for less than 2 hours	K	A-F		
Reactivity changes in the fuel pool					
E2-04	Disturbances in the boron concentration (only PWR)	R	A-F		Note: Only relevant in case of boron credit in the storage design.
E2-05	Most unfavourable misloading of the fuel pool or transport and storage cask with a most reactive fuel element	R	A-F		
Level of defence 3					
Reduced heat removal from the fuel pool					
E3-01	Loss of two trains of the fuel pool cooling system for a longer period (> 30 min.)	K	A-F		Additional boundary condition: For the safety demonstrations, grace times and repair possibilities are taken into account.
Loss of coolant from fuel pool					
E3-02	Leak in the fuel pool or in a connecting pipe (leak cross section ≤ DN 50)	K B	A-F		
E3-03	Leak in the reactor cavity with opened	K	E		

No.	Fuel element handling and storage events for PWRs and BWRs	Protection goals concerned	Opera-tional phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
	refuelling slot gate	B			
E3-04	Drop and impact of loads with potential risk for safety-relevant installations	Design requirement	A-F		Additional boundary condition: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components”, Section 2.2.4 (Module 10).
E3-05	Internal leak in heat exchangers of the fuel pool carrying coolant	K B S	A-F		
Loss of energy supply					
E3-06	Loss of offsite power for more than 2 hours	K S	A-F		
Reactivity changes in the fuel pool					
E3-07	Water/steam ingress in the spent fuel dry storage facility	R B	A-F	Specification of the acceptance criteria: $k_{eff} < 0.98$	
E3-08	Geometry changes due to earthquake (fuel pool, spent-fuel dry storage facility)	R K B	A-F		
E3-09	Drop of a fuel element into the fuel pool	R	A-F		Additional boundary condition: A dropped-down fuel element is lying on the storage racks or standing directly adjacent to a storage rack.
E3-10	Misloading of the fuel pool or the transport and storage cask with more than one fuel element	R VM	A-F	Criteria for potential preventive measures: See “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant	

No.	Fuel element handling and storage events for PWRs and BWRs	Protection goals concerned	Opera-tional phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
				Structures, Systems and Components", Section 4.2.3 (Module 10).	
E3-11	Boron dilution in the fuel pool (only PWR)	R	A-F		Note: Only relevant in case of boron credit in the pool design.
Events during handling and storage of fuel elements and heavy loads					
E3-12	Fuel element damage during handling	S	A-F		Additional boundary condition: Damage of all fuel rods at exterior side of a fuel element is postulated. Note: The analysis serves to verify that the release into the environment resulting from the release of radionuclides in the containment without loss of coolant is sufficiently limited.
E3-13	Drop of the fuel element transport cask	Design requirement	A-F		Additional boundary condition: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components", Section 2.2.4 (Module 10).
E3-14	Drop of heavy loads including fuel element transport cask onto the fuel pool	Design requirement	A-F		Additional boundary condition: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components", Section 2.2.4 (Module 10).
Internal event					
E3-15	Plant-internal fire with impacts affecting more than one redundancy	Design requirement	A-F		Additional boundary condition: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe

No.	Fuel element handling and storage events for PWRs and BWRs	Protection goals concerned	Opera-tional phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
					Operation of Plant Structures, Systems and Components", Section 2.2.1 (Module 10).
E3-16	Plant-internal fire including filter fire and explosions	S	A-F		Additional boundary condition: Performance of analyses on fires and explosions affecting components or system areas with high activity release potential.
E3-17	Plant internal flooding	Design requirement	A-F		Additional boundary condition: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components", Section 2.2.2 (Module 10).
E3-18	Component failure with potential impact on safety-relevant installations	Design requirement	A-F		Additional boundary condition: - Details on the leak or break assumptions and on safety demonstrations are included in Annex 2. - See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components", Section 2.2.3 (Module 10).
E3-19	Electromagnetic internal events (except lightning)	Design requirement	A-F		Additional boundary condition: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components", Section 2.2.5 (Module 10).
E3-20	Collision of vehicles at the plant site with safety-relevant, structures or components	Design requirement	A-F		Additional boundary condition: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and

No.	Fuel element handling and storage events for PWRs and BWRs	Protection goals concerned	Opera-tional phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
					Components", Section 2.2.6 (Module 10).
E3-21	Plant-internal explosions, including radiolysis gas explosions in systems and components	Design requirement	A-F		Additional boundary condition: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components", Section 2.2.8 (Module 10).
External event					
E3-22	Earthquake (including consequential impacts)	S Design requirement	A-F		Additional boundary condition: - Postulation of failure of that container which represents all others radiologically. See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components", Section 3.2.3.2 (Module 10).
E3-23	Extreme site-dependent events, such as ambient temperatures, flood, storm, snow, ice, lightning, external fire and, where applicable, other site-dependent events to be postulated, such as rock damage, ground settlement, mudslides, biological impacts in cooling water intakes (e.g. mussel growth, jellyfishes)	Design requirement	A-F		Additional boundary condition: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components", Section 3.2.3 (Module 10).
E3-24	Impairment of heat removal by flotsam and ship accidents	Design requirement	A-F		Additional boundary condition: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components", Section 3.2.2.1 (Module 10).
E3-25	Electromagnetic external events (except lightning)	Design requirement	A-F		Additional boundary condition: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and

No.	Fuel element handling and storage events for PWRs and BWRs	Protection goals concerned	Opera-tional phase	Additional comments on the acceptance criteria	Additionally considered boundary conditions and notes
					Components", Section 3.2.2.2 (Module 10).
Level of defence 4					
Level of defence 4a					
External event					
E4a-01	Impacts of multi-unit plants or neighbouring plants	Design requirement	A-F		Additional boundary condition: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components", Section 2.2.7 (Module 10).
E4a-02	Aircraft crash	Design requirement	A-F		Additional boundary condition: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components", Section 3.2.1.1 (Module 10).
E4a-03	Plant-internal explosion	Design requirement	A-F		Additional boundary condition: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components", Section 3.2.1.2 and 3.2.1.3 (Module 10).
E4a-04	Intrusion of hazardous substances	Design requirement	A-F		Additional boundary condition: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components", Section 3.2.1.4 (Module 10).

Annex 1

Principal classification of load levels according to levels of defence

N o t e: In the present list, events are classified according to the levels of defence defined in the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria” (Module 1). The criteria in the “Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System“ (Module 4) refer to the events classified according to these different levels of defence. Compared with this, load cases and load case classes (these are dimensioning or design load cases, assembly load cases, normal and anomalous operational load cases, test load cases and incidents) are classified in the KTA standards according to load levels (0, A, B, C, D, P or 0, 1, 2, 3 (for the containment) to which the permissible stresses and deformations are assigned without having made reference to events or levels of defence so far. In order to be able to associate the general criteria in the “Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System“ (Module 4) with the detailed requirements of the KTA standards, the respective load levels of the KTA standards are to be assigned to the events of the different levels of defence under consideration of the specifications in the “Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System“ (Module 4). As a guidance, the following matrix includes a principal classification of load levels according to the levels of defence. Therefore, the load levels for the reactor coolant pressure boundary, the external systems and the containment defined in the respective KTA standards (3201.2, 3211.2 and 3401.2) are classified there according to the levels of defence. For the columns “Reactor coolant pressure boundary” and “External systems” of the matrix, the first level mentioned within a line always represents the normal case in case of multiple mentions of load levels. The other levels mentioned can or must be used if there are specific cases which are specified by the notes on the right. For the reactor coolant pressure boundary, the significance of the load levels and the associated sets of criteria is currently presented in KTA Safety Standard 3201.2. Accordingly, KTA Safety Standard 3211.2 is to be referred to for the external systems. For the containment, the applicable load levels are determined in dependence of the load cases to be considered according to the load combinations to be considered so that in the matrix, no notes are used for the containment. The load levels assigned to the different load combinations as well as the more detailed related criteria for the containment are stated in KTA Safety Standard 3401.2.

A1 (1) The classification of load levels according to levels of defence is performed plant-specifically such that all systems, including the system transitions and components, are considered. Starting point is the compilation of load conditions for each system which is structured according to the levels of defence. On the basis of this compilation, impacts and the associated event- and safety-related task are defined for each system section as well as the component-specific requirements for safety demonstrations with regard to function, support stability and barrier effectiveness.

		Load levels		
		Reactor coolant pressure boundary[1]	External systems[2]	Containment[3]
Level of defence		Design level 0	0	0
1		A/P	A/P	1/2
2		B[8]	B[8]	1/2
3[11]		C[4,9,11]/D[5]	C[9,11]/B[10]/D[5]	1/2/3
4	a	D/C[6]	D[12]	3[13]
	b	[7]	[7]	3
	c	[7]		

[1] Criteria of Module 4, Section 2 are fulfilled.

[2] Criteria of Module 4, Section 3 are fulfilled.

[3] Criteria of Module 4, Section 7 are fulfilled.

[4] Except for large leak within the containment.

[5] Large leak within the containment: Not permissible if, subsequently, use of the component is required for the control of the accident.

[6] For operational transients with postulated failure of the reactor scram system.

[7] For levels of defence 4b and 4c, no criteria are imposed with regard to the load levels. There are criteria for accident management measures for levels of defence 4b and 4c in "Safety Criteria for Nuclear Power Plants: Criteria for Accident Management" (Module 7).

[8] Including fatigue protection for tests on safety installations and equipment.

[9] For loads resulting from the event only if functional requirements are not impaired; if required, functional capability is verified or load is restricted to level B.
Regarding earthquakes, the classification according to load levels is checked site-specifically under consideration of the magnitude of the design earthquake.

[10] For loads resulting from the operation of the safety system.

[11] For load case “safe shutdown earthquake”, the classification according to load levels considers the large population of the components concerned.

[12] Functional capability is verified for components necessary for the control of the event.

[13] For load cases “aircraft crash” and “explosion blast wave”, the integrity for the undisturbed areas of the containment is demonstrated.

Annex 2

Postulated leak cross sections and breaks in the reactor coolant pressure boundary and in the external systems and on components

1 Principles and prerequisites

1 (1) The leak cross sections are postulated values and refer to the open cross-sectional area A of the respective pipe or line.

N o t e: The criteria in Sections 2.1 and 3 are classified according to the following acceptance targets:

- Maintenance of fuel element cooling by compensating the loss of coolant (design of the emergency cooling systems),
- ensuring the possibility of shutdown and cooling of the reactor core geometry,
- prevention of consequential damage affecting the reactor coolant pressure boundary, building parts and adjacent systems necessary for the control of the event, and
- maintenance of the barrier integrity of the containment, for BWRs also maintenance of the function of the pressure suppression system.

For the fulfilment of these acceptance targets, further criteria are applicable in addition to the criteria stated in these sections, see, in particular, in the "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Operation of the Reactor Core" (Module 2) and in the "Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors" (Module 3)

1 (2) The application of this annex requires the fulfilment of the criteria of the "Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System" (Module 4), Sections 2 and 3 as well as 4.1 to 4.3.

1 (3) For sections of high-energy piping systems of the reactor coolant pressure boundary and the external systems between the containment and the external isolation device, for which no consequential damage is postulated in the safety demonstrations, the criteria according to the "Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System" (Module 4), Section 4.6 apply.

1 (4) For the piping systems not dealt with in the following, a 2A break is postulated.

2 Reactor coolant pressure boundary of PWRs

2.1 Main coolant line including connecting lines DN > 200

Maintenance of fuel element cooling by compensating the loss of coolant (design of the emergency cooling systems)

2.1 (1) For the analysis of the emergency core cooling effectiveness, leak cross sections in the main coolant lines of up to 2A inclusively are taken as a basis (A = open cross-sectional area). The emergency cooling systems are designed accordingly.

Ensuring the possibility of shutdown and cooling of the reactor core geometry

2.1 (2) As load assumption for the internals of the reactor pressure vessel and the reactor core, a fast opening leak (linear opening behaviour, opening time 15 ms) with a cross section of 0.1 A in the main coolant lines is postulated for different leak positions.

Prevention of consequential damage

2.1 (3) For the determination of the impacts from jet and reaction forces on pipes, components, component internals and building parts, a leak with a cross section of 0.1 A of the respective line and static discharge flow for different leak positions to be considered is postulated. This also applies to the determination of releases or debonding of material resulting from jet forces with regard to potential impairment of emergency cooling by these materials, postulating the most unfavourable leak positions and sizes (≤ 0.1 A).

2.1 (4) For the control of the consequences (pressure build-up in the reactor cavity) of a postulated leak with a 0.1 A cross section between reactor pressure vessel and biological shield, provisions are made – as far as required – as e.g. guard pipes in the area of the penetrations of the main coolant lines through the biological shield.

2.1 (5) For demonstration of the support stability of the components, reactor pressure vessel, steam generator, main coolant pumps and pressuriser, the following postulations apply:

The support stability of these components is ensured for the static equivalent force P_{ax} superposed with the dead weight of the component:

$P_{ax} = 2 \cdot p \cdot A$
with
p = operating pressure at full power
A = open cross-sectional area

Point of force application: centre of the pipe cross section in the area of the nozzle circumferential weld.

Effect: nozzle axis in most unfavourable direction for the support stability of the component.

This force is only acting on one nozzle each. The support stability is demonstrated separately for each nozzle.
N o t e: For the steam generator, support stability is ensured in the same way as for the connection to the secondary circuit. This is dealt with under the leak postulates of the main stream and feedwater lines.

2.1 (6) Design pressure and design temperature for fault-proof electrical installations are defined for a leak cross section of 2A in the main coolant lines.

Maintenance of the barrier integrity of the containment

2.1 (7) For the determination of the pressure design of the containment and the determination of the pressure differences within the containment, leak cross sections up to 2A inclusively in the main coolant lines are taken as a basis.

2.2 Reactor pressure vessel

2.2 (1) Regarding the anchorage of the reactor pressure vessel (limitation of pressure load on support structures), the load on the RPV internals and the design of the emergency core cooling system, a leak in the reactor pressure vessel with a size of about 20 cm2 (geometric cross section: circular) below the upper edge of the reactor core is also postulated.

2.2 (2) The design of the RPV internals and of the protection measures for the containment also consider the consequences of a sudden break of a control rod drive or mechanism nozzle with the maximum possible leak cross section in the reactor pressure vessel.

2.3 Steam generator tubes

2.3 (1) The loads occurring during a postulated main steam or feedwater line break or a stuck-open secondary-side safety valve on the steam generator tubes due to static and transient loading (blast wave, flow forces, static pressure differences via the steam generator tubes) are determined. It is demonstrated that the steam generator tubes withstand these loads.

2.3 (2) Regarding the accident analysis for the main steam line break, however, the failure of some few steam generator tubes is generally postulated as random failure and not as additional failure resulting from the main steam line break which is considered enveloping by assumption of the complete rupture (2A) of a steam generator tube in the steam generator affected. In this case, a single failure at another location is not postulated in this accident analysis.

2.3 (3) Regarding the main steam line break outside the external isolation valve with additionally postulated “non-closure of the isolation valve”, steam generator tube failure is not postulated if the above-mentioned load verification has been performed according to subsection 2.3 (1).

2.3 (4) For feedwater line break, steam generator tube failure is not postulated.

2.3 (5) If postulating subcritical cracks or the rupture of a small-bore line, no additional steam generator tube failure is superposed.

3 Reactor coolant pressure boundary of BWRs

Maintenance of cooling of the fuel elements by compensation of loss of coolant (design of the emergency cooling systems)

3 (1) The analysis of the effectiveness of emergency core cooling and the design of the emergency cooling systems are based on the following leak cross sections:

a) in the main steam and feedwater lines up to 2A, and
b) in the reactor pressure vessel, on the one hand, 80 cm2 (geometric cross section: circular) below the upper edge of the reactor core, on the other hand, the maximum possible leak cross section resulting from the break of a core instrumentation nozzle or the housing tube of a control rod drive or the weld between housing tube and RPV.

Ensuring the possibility of shutdown and cooling of the reactor core geometry

3 (2) Load assumption for internals of the reactor pressure vessel and the reactor core is a fast opening leak (linear opening behaviour, opening time 15 ms) with a cross section of 2A in the main steam and feedwater lines for different leak positions and leaks according to (1) b).

Prevention of consequential damage

3 (3) Regarding the load assumption for the jet and reaction forces on pipes, components, component internals and building parts, a leak with a cross section of 0.1 A of the respective line and static discharge flow for different leak positions to be considered is postulated. This also applies to the determination of releases or debonding of material resulting from jet forces with regard to potential impairment of emergency cooling by these materials, postulating the most unfavourable leak positions and sizes (≤ 0.1 A).

3 (4) For the control of the consequences (pressure build-up in the gas space of the wetwell) of a postulated leak in the pressure relief pipe with a 0.1 A cross section between wetwell ceiling and the leak area of the pressure relief pipe, provisions are made – as far as required – as e.g. guard pipe around the pressure relief pipe.

3 (5) Regarding dynamic loads, incoming blast waves resulting from breaks in line areas behind the external isolation valve (outside the containment) or postulated as consequence of an external event are considered in the design basis. Here, a guillotine break (2A break) with linear opening behaviour and an opening time of 15 ms is postulated as input parameter for the calculation. With this assumption, analyses of dynamic loads resulting from subcritical cracks become unnecessary.

3 (6) For verification of the support stability of the reactor pressure vessel, the following postulations apply:

The support stability of the components is ensured for the static equivalent force P_{ax} superposed with the dead weight of the component:

$$P_{ax} = 2 \cdot p \cdot A$$

with
p = operating pressure at full power
A = open cross-sectional area

Point of force application: centre of the pipe cross section in the area of the nozzle circumferential weld.

Effect: nozzle axis in most unfavourable direction for the support stability of the component.

This force is only acting on one nozzle each. The support stability is demonstrated separately for each nozzle.

3 (7) The anchorage is dimensioned such that also the leaks postulated according to 3 (1) b) are covered.

3 (8) For the determination of design pressure and design temperature for fault-proof electrical installations, a leak cross section of 2A in the main steam and feedwater lines is taken as a basis.

Maintenance of the barrier integrity of the containment

3 (9) For the determination of the design pressure and the determination of the pressure differences within the containment as well as the dimensioning of the pressure suppression system, leak cross sections in the main steam and feedwater lines of up to 2A inclusively are taken as a basis.

4 External systems

4.1 Main steam and feedwater lines of PWRs

4.1 (1) For the main steam and feedwater lines between steam generator and valve station outside the containment, leaks resulting from subcritical cracks are postulated. These were calculated on the basis of fracture mechanics or limited to 0.1 A.

For these leak cross sections determined on the basis of fracture mechanics, the following general verification steps are considered:
- The leak detection systems are designed such that a specified leakage rate is reliably identified.
- For the postulated through-wall crack at any arbitrary location, the methods according to fracture mechanics show, on the one hand, that for the impacts from processes on level of defence 1, there is a sufficiently large crack opening area for the specified leakage rate. On the other hand, it is shown that for all impacts from processes and events on levels of defence 1 to 3, the largest possible crack length for this crack opening area is subcritical (this crack length is longer than the crack length relevant for the detectability of the leak).
- For verification of the permissibility of the impacts from the subcritical crack on the system affected, it is superposed with the impacts resulting from the relevant event on levels of defence 2 and 3.
- For each verification step, sufficient margins are chosen which consider the respective uncertainty of the approximation of physical phenomena (e.g. leakage rate for leak detection) with simplified methods (e.g. simplifications of fracture mechanics, determination of elastic internal forces and moments for piping systems with elastic-plastic behaviour).

4.1 (2) For the determination of the impacts from jet and reaction forces on the main steam and feedwater lines between steam generator and valve station outside the containment, a leak with a cross section of 0.1 A of the respective line and static discharge flow is postulated.

4.1 (3) Regarding dynamic loads of the main steam and feedwater lines, incoming blast waves resulting from breaks in line areas behind the first isolation valve outside the containment or postulated as consequence of an external event are considered in the design basis. Here, a guillotine break (2A break) with linear opening behaviour and an opening time of 15 ms is postulated as input parameter for the calculation. With this assumption, analyses of dynamic loads resulting from subcritical cracks become unnecessary.

4.1 (4) For verification of the support stability of the steam generator, the following postulations apply regarding the connection to the secondary circuit:

The support stability of the steam generator is ensured for the static equivalent force P_{ax} superposed with the dead weight of the component:

$$P_{ax} = 2 \cdot p \cdot A$$

with
p = operating pressure at full power
A = open cross-sectional area

Point of force application: centre of the pipe cross section in the area of the first connecting weld.

Effective direction: nozzle axis in most unfavourable direction for the support stability of the component.

This force is only acting on one nozzle each. The support stability is demonstrated separately for each nozzle.

4.1 (5) The impacts of a main steam line break and a consequential cold-water transient on reactivity behaviour and on the change of pressure and temperature in the reactor as well as the resulting loads on the reactor pressure vessel with its internals are controlled.

4.2 Other external systems of PWRs and BWRs

4.2 (1) For pipes of the external systems other than those mentioned in Section 4.1, the following leak and break assumptions apply as far as these pipes are located in the reactor building:
- Subcritical cracks in the welds. The resulting leak cross sections were calculated on the basis of fracture mechanics or limited to 0.1 A.
- For pipes with nominal diameters equal to or larger than DN 50, additionally supercritical (instable) circumferential cracks at highly stressed circumferential welds if one of the criteria a1) or a2) applies:

a)1.operating pressure[10] ≥ 20 bar **or**
a)2.operating temperature[1] ≥ 100 °C

and the following two criteria are fulfilled additionally:
b) operating time more than 2 % and
c) nominal operating stress larger than 50 N/mm^2.

4.2 (2) If a guillotine break is postulated in accordance with the criteria mentioned, the proceeding with regard to the consequential effects is as follows:
- For the determination of differential pressures or jet forces on building parts, unimpeded discharge flow is postulated.
- For the calculation of an internal blast wave for determination of the loads of internals, unimpeded discharge flow is postulated.
- For the determination of reaction forces, limitations of the leak area due to constructive measures may be considered.

4.2 (3) For leaks at the wetwell of the boiling water reactor, the guillotine break of the largest connecting pipe is postulated.

4.2 (4) For pipes with a diameter smaller than DN 50 and all pipes outside the reactor building, double-ended breaks are postulated in general and the permissibility of all consequences to be considered is demonstrated.

5 Vessels, valve and pump casings

Bursting of vessels (other than reactor pressure vessel), heat exchangers and valve and pump casings is generally postulated.
For those vessels (other than reactor pressure vessel), heat exchangers and valve and pump casings, including the pertinent casing of the circulator turbine, being part of the reactor coolant pressure boundary or the external systems and for which the respective break preclusion and break resistance demonstrations (see "Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System", Section 8 (Module 4) were presented, the respective leak and break postulates of the connecting pipes are assumed. For vessels, heat exchangers and other components with several connections, the most unfavourable leak is considered in dependence of the acceptance target, taking into account the leak and break postulates for the selected connecting pipe.

---

[10] In load level A, see Annex 1

D

MODULE 4
"Safety Criteria for Nuclear Power Plants:
Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System"

Contents

1 Objectives and scope

This guidance text contains the safety-related criteria for the design, manufacturing and operation of the reactor coolant pressure boundary, the pressure-retaining walls of components of the external systems and the containment system. Further, it contains criteria for pipe guards for piping systems.

N o t e: Criteria regarding the function of the components mentioned here are included in the "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components" (Module 10, in Section 5.2).

2 Reactor coolant pressure boundary

2.1 Scope

2.1 (1) The following criteria are applied to the reactor coolant pressure boundary (RCPB) of light-water reactors made of metallic materials.

2.1 (2) In the case of pressurised water reactors, the reactor coolant pressure boundary comprises the following components. Their internals are only to be considered as part of the RCPB if they are pressure–retaining and if their failure may lead to an impairment of the barrier integrity of the RCPB.

a) Reactor pressure vessel,
b) primary side of the steam generators (SGs), including SG tubes,
c) pressuriser,
d) main coolant pumps,
e) connecting pipes between the above components, including parts of any valve belonging to the same pressure zone,
f) pipes branching off from the above components and the pipes they connect, including the parts of valves belonging to the same pressure zone up to and including the first isolation valve,
g) pressure-retaining walls of the control element drives and core instrumentation,
h) integral areas of component support structures and welded attachments.

2.1 (3) The secondary shell of the steam generators including the feedwater inlet and main steam exit nozzles up to the pipe-connecting welds, but not the minor nozzles and nipples, shall also be treated as the RCPB regarding material selection, design principles, quality assurance, manufacturing control and in-service inspections.

2.1 (4) In the case of boiling water reactors, the reactor coolant pressure boundary comprises the following components. Their internals are only to be considered as part of the RCPB if they are pressure–retaining and if their failure may lead to an impairment of the barrier integrity of the RCPB.

a) Reactor pressure vessel,
b) the pipes belonging to the same pressure zone as the reactor pressure vessel including the installed parts of valves up to and including the first isolation valve if these pipes penetrate the containment up to and including the first isolation valve located outside the containment,
c) pressure-retaining walls of the control rod drives, the core instrumentation and the reactor recirculation pumps,
d) integral areas of component support structures and welded attachments.

2.1 (5) Components of isolation valves required for the isolation of the pressure chamber are considered as part of the reactor coolant pressure boundary.

2.1 (6) The following criteria do not apply to pipes and components smaller or equal to DN 50. For such pipes and components with small nominal diameters, criteria are defined in Section 5.

2.2 Principles of basic safety in connection with design and manufacturing

2.2. (1) The basic safety of the reactor coolant pressure boundary which precludes any catastrophic failure of a plant component as a result of manufacturing defects is ensured by fulfilment of the following criteria under consideration of the operating medium:

- use of high-quality materials, in particular with regard to toughness and corrosion resistance,
- conservative limitation of stresses,

– prevention of stress peaks by optimised design and construction, and
– assurance of the application of optimised manufacturing and testing technologies.

This requires the knowledge and assessment of possibly existing defects.
N o t e: See ”Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1), subsection 3.4 (5).

2.2. (2) Further, the structural layout of all components is such that the criteria for a design not leading to an increase of loads/stresses, meeting the specific requirements for the materials, manufacturing and functions as well as for a maintenance-friendly design are fulfilled and that the non-destructive tests during manufacture and at the place of installation as well as the non-destructive in-service inspection can be performed to a sufficient extent. This applies, in particular, to the welds and the base material of cladded material areas.

2.3 Design

2.3.1 Principles

2.3.1 (1) For ensuring the integrity of the components, a design concept exists which considers the principles presented in this section.

2.3.1 (2) The integrity demonstrations as part of the design are performed such that the required safety distances are shown for all impacts of specified normal operation and from events of levels of defence 3 and 4a over the entire planned lifetime. Potential ageing-induced damage mechanisms and changes of the material properties by impacts such as temperature and irradiation, which may occur during operation, are taken into consideration. The main ageing-induced damage mechanisms are fatigue, relaxation, wear and different types of corrosion. Moreover, synergisms of different mechanisms are taken into consideration.

2.3.1 (3) The design of components is based on load cases, beginning with impacts. The load cases are derived, in particular, from specified plant operation, from operating experience and from the events postulated according to the “Safety Criteria for Nuclear Power Plants. Events to be Considered in Pressurised and Boiling Water Reactors” (Module 3) and cover the resulting impacts. The load cases and their combinations are specified and completely described according to their characteristics and frequency. Load case combinations are postulated if the events a n d / o r operating phases to be combined may be causally connected or if their simultaneous occurrence has to be postulated according to probability considerations. The impacts resulting from these load cases are described component-specifically also under consideration of the technology of adjacent systems. Impacts from installed components are considered in the integrity demonstration (e.g. with regard to dead weight, support stability, mechanical impacts, thermal-hydraulic conditions) as far as they may influence the integrity of the pressure-retaining walls.

2.3.1 (4) For preventing excess of the pressure permissible on the respective level of defence, reliable systems are provided. The required systems for pressure limitation and overpressure protection can discharge the media to be considered reliably on all levels of defence.

2.3.2 Material selection

2.3.2 (1) By material selection and adequate structural design, welding and heat treatment, it is ensured for the reactor coolant pressure boundary that throughout the planned lifetime of the plant, a sufficiently strong and tough material condition is maintained such that the loads occurring during specified normal operation and in case of events on levels of defence 3 and 4a can reliably be borne.

For the demonstration of the specified strength and toughness, manufacturing in accordance with the specifications is demonstrated for all materials with certificates.

For ferritic steels, a sufficiently high level of upper shelf toughness is given. For loads from stationary operating conditions on levels of defence 1 and 2, the lowest temperature loading exceeds the NDT temperature such that a defined minimum toughness ensured. This applies to base material, weld material and heat-affected zones.

2.3.2 (2) In combination with the selected construction and the processing techniques applied, the materials used have sufficient resistance against corrosion and other ageing effects under the operating conditions. The water qualities required for corrosion resistance during specified normal operation (levels of defence 1 and 2) are specified. The water quality is monitored and deviations from the specified parameters are detected at an early stage so that disadvantageous impacts on the components are prevented.

2.3.2 (3) The materials are selected under consideration of the other criteria for materials (see Sections 2.2 and 2.3) such that an activation of the materials and their corrosion products remains as low as possible.

2.3.2 (4) Component parts with sealing and / or sliding function show sufficiently high chemical, mechanical and physical resistance under the conditions of specified normal operation (levels of defence 1 and 2). Unavoidable corrosion and abrasion products as well as released substances are

– due to their chemical composition
– or due to measures taken or installations installed against their insertion into the reactor coolant or their local accumulation

radiologically irrelevant and cause no damage of the components by corrosion.

2.3.3 Construction and arrangement

2.3.3 (1) The components of the reactor coolant pressure boundary are arranged and installed such that, in case of events on levels of defence 3 and 4a, no consequential damages at other safety-relevant plant components can occur which may endanger the fulfilment of the safety function of these components

Note: For the impacts to be considered, see also “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components“ (Module 10, Section 2).

2.3.3 (2) For all components of the reactor coolant pressure boundary, adequate possibilities for inspections and in-service inspections are available. In areas with increased radiation levels, heat insulations at the components to be inspected are designed such that they can fastly be removed and remounted, if required. For better reproducibility of the test parameters and test boundary conditions and for better comparability of the test results as well as for limitation of the radiation exposure of the personnel, mechanisation of the tests is made possible.

2.3.3 (3) Bolted joints are designed such that the necessary tightness is reached in a reliable manner. Their design is qualified and their suitability demonstrated on the basis of technical experience. They are monitored adequately so that leakages that might occur are detected early enough to prevent impermissible consequences.

2.3.3 (4) Regarding pipes branching off, the isolation valve is located as near as possible to the branch-off point.

2.3.3 (5) Installed components of isolation devices are designed such that they show the necessary load-bearing capacity for ensuring the sealing function.

2.3.3 (6) Pipe laying and spatial arrangement of the valves ensure that accumulations of condensate in steam-carrying plant components are prevented by drainage.

2.3.4 Strength design

2.3.4 (1) The integrity demonstrations prove that margins to the occurrence of failure types to be postulated are observed. The stresses caused by mechanical and thermal loads in the components are limited such that for the respective level of defence a safety distance to the occurrence of postulated failure types is given according to the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1). In case of uncertainties about the state of knowledge on damage mechanisms, these are considered by respective safety margins or

conservative safety demonstrations. For the components, preventive measures were taken against failure due to the following mechanisms:
a) plastic instability,
b) global deformation,
c) ratcheting,
d) fatigue, and
e) unstable crack propagation,
f) elastic instability.

2.3.4 (2) The necessary safety distances for the stresses resulting from these impacts are defined for the different levels of defence as follows:
a) The stress limits of levels of defence 1 and 2 ensure that the balance between stresses and impacts, including the safety margins specified according to the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1), subsection 3.1 (2), is achieved such that no global plastic deformations, no elastic instability, no break, no failure due to ratcheting and no failure due to fatigue occur. The safety distances are determined such that in case of stresses from internal pressure, weight, fluid dynamics and other, quasistatic impacts, the load-bearing cross sections remain in the range of elastic material behaviour, except for locally limited areas. For additionally acting stationary and dynamic impacts from operating conditions of levels of defence 1 and 2, the safety distances are defined such that, in addition, a failure due to ratcheting and fatigue is not to be postulated either.
b) The stress limits of levels of defence 3 and 4a ensure that the balance between stresses and impacts, including the safety margins to be considered (see “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1), subsection 3.1 (2)), is achieved such that a failure due to plastic or elastic instability or due to unstable crack propagation is excluded. The safety distances are selected such that in case of stresses from internal pressure, weight, fluid dynamics and other additional loads from external events being similar regarding their characteristics, the plastic deformations remain limited. The demonstration for the exclusion of failures due to unstable crack propagation includes, in addition, the impacts from restrained thermal expansion.
c) For events on levels of defence 3 and 4a, plastic deformations are limited to the area of geometric discontinuities. For geometrically simple component parts (e.g. pipes), plastic deformations of the entire cross section are permissible in case of dynamic loads; however, the resulting deformations clearly remain below the uniform elongation of the material under consideration of the influence of multiaxiality, which may lead to a restricted deformability and other effects which may increase the deformations occurring.

2.3.4 (3) For events on levels of defence 3 (e.g. design earthquake) and 4a, whose management requires the function of parts of the RCPB, the stress limits for the required components are defined such that the operability of these components remains ensured.

2.3.4 (4) The integrity demonstration is performed by experiments or calculations or in combination of these methods. An acceptance target is specified and its fulfilment is demonstrated with validated methods. The applicability of the boundary conditions of the computational methods or experiment to the boundary conditions of the components or systems for which safety demonstrations are required is demonstrated. The observance of the above mentioned safety distance between acceptance target and failure or occurrence of a state to be prevented is shown.
N o t e: Regarding criteria for experimental demonstration and the validation of methods see also “Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation“ (Module 6).

2.4 Manufacturing

2.4.1 Principles

2.4.1 (1) The quality criteria to be fulfilled for ensuring integrity are defined and considered in the planning of the manufacturing process.

2.4.1 (2) Manufacturing is performed with qualified methods and by qualified manufacturers.

2.4.1 (3) The manufacturing process is monitored and documented such that deviations from specified quality criteria are identified and traceability of the deviations with regard to their causes is possible. Additional measures taken for achieving the criteria are documented.

2.4.1 (4) For welding materials and supplies, certification tests or qualification tests are performed. The manufacturer verifies by means of corresponding welding procedure qualification tests that he surely masters the envisaged welding procedures.

2.4.1 (5) Weld cladding on ferritic components is designed such that the base material can be subjected to ultrasonic examination methods from at least two surfaces.

2.4.2 Destructive in-process tests

2.4.2 (1) By means of tests on product forms, it is demonstrated that the specified properties of the chemical composition, toughness, structural strength and corrosion resistance are present across the wall thickness.

2.4.2 (2) The mechanical-technological properties are demonstrated for each product form (component-wise or batch-wise) which includes the following:
a) representatively, the different deformation directions at several sampling points, and
b) all transformation and heat treatments taking place during the manufacturing process.

2.4.2 (3) For verification of the quality characteristics of production welds, production weld tests are performed. It is permissible to combine the production weld tests with welding procedure qualification tests.

2.4.2 (4) For weld-cladded product forms, proof is given that there are no underclad cracks. In justified cases, this may also be done by non-destructive tests of the components.

2.4.3 Non-destructive in-process tests

2.4.3 (1) For all product forms and welds, including butterings, provided for the reactor coolant pressure boundary, the volume and surfaces are subjected to non-destructive tests with sufficient detectability of defects.

A weld cladding is tested for adhesion, underclad cracks and defect-free condition of the surface. The test scope with regard to underclad cracks is defined under consideration of subsection 2.3.2 (4).

The techniques and parameters for the volumetric examination are selected such that all safety-relevant flaws are detected. This requires that the examinations are performed with sensitivities which allow detection of indications with dimensions clearly below the size of safety-relevant flaws. In this respect, flaws oriented perpendicular to the principal stress directions (operating stresses) are considered by selecting qualified techniques and parameters (such as sound propagation directions).

The permissible limits for indications in the volume are generally defined such that technically relevant changes of the indication dimension by impacts from operation are not to be expected.

The surface tests cover all flaw orientations of the test geometry. Crack-like indications at the surface are not permissible. Methods for removal of surface crack indications are qualified regarding the damage mechanisms to be considered during operation. Application according to the specification is monitored and confirmed by tests.

2.4.3 (2) Type, timing and scope of the non-destructive tests are defined depending on the product form and component. The test for assessment of the relevant quality conditions of the product forms and components is performed after the last heat treatment.

2.4.3 (3) At the end of the manufacturing process, all components of the reactor coolant pressure boundary are subjected to a pressure test at a test pressure higher than the design pressure (initial pressure test).

2.4.3 (4) Within the framework of specified tightness requirements, leak tests are performed (e.g. overall system, steam generator tubes).

2.5 Operation

2.5.1 Principles

2.5.1 (1) For maintaining the barrier function, a monitoring and testing concept is established for

– checking compliance with the design boundary conditions and prerequisites, and
– ensuring operating experience feedback and its use in ageing management.

The boundary conditions regarding spatial layout, anchoring, function of supports, valves, pumps and internals on which the design of the components and systems is based are documented (e.g. free path lengths, displacements, deflections, clearances for high-temperature systems). During commissioning and, as far as required, after interferences (e.g. maintenance measures), compliance with the boundary conditions is checked. Impermissible deviations from these boundary conditions are prevented or identified in sufficient time such that no impacts on the integrity of the pressure-retaining walls take place.

2.5.1 (2) Operating parameters which are significant for the integrity of the components (e.g. mechanical and thermal loads, water quality) are monitored and checked for plausibility under consideration of the respective postulated system state. Moreover, monitoring for leaks is provided which ensures the detection and sufficiently precise localisation of leakages.

2.5.1 (3) The operating conditions in the operating phases of low-power and shutdown operation (operating phases B - F) and during functional tests are specified with regard to the impacts influencing the integrity of components. The fulfilment of these requirements is ensured by the operating instructions (e.g. temperature, water chemistry). Deviations from these specifications are prevented or identified in sufficient time such that no impacts on the integrity of the pressure-retaining walls take place.

2.5.1 (4) Components or component areas for which relevant stresses are to be expected according to analyses or due to operating experience with regard to ageing-induced damage mechanisms are included in a monitoring and testing concept.

2.5.1 (5) It is ensured that on levels of defence 1 and 2 the amounts of hydrogen (radiolysis gases, added hydrogen) which can permeate from the circuits into a non-inerted atmosphere of the containment remain limited such that an explosive accumulation with potential for consequential damage is precluded.

N o t e: See also “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components“ (Module 10, in Section 2.2.8.2).

2.5.1 (6) Accumulations of non-condensable gases

a) at the highest point of the cooling circuit,
b) in components with no or only small through-flow

are recorded with regard to potential thermal loads on the pressure-retaining wall and potential malfunctions of the system. They are assessed with regard to their safety-related consequences.

2.5.1 (7) If relevant indications are identified during the examinations, proceeding takes place according to Section 8.

2.5.1 (8) For systematic identification, observation or prevention of ageing impacts on the integrity of the components of the pressure-retaining walls, an ageing management system is implemented.

2.5.1 (9) The technical systems and auxiliary equipment as well as the handling procedures employed for work on the components of the reactor coolant pressure boundary (e.g. on threaded joints during tests and cleaning) are qualified such that detrimental impacts on the components are prevented or identified in sufficient time such that no impermissible impacts on the integrity of the pressure-retaining walls take place.

2.5.1 (10) The testing concept is updated with regard to the remaining operating life well before end of operation. Planned tests are scheduled such that there will be a gain in safety.

2.5.2 In-service leak and pressure tests

2.5.2 (1) After each reclosure of a pressure-retaining system, an integral leak test is performed under a defined reference condition.

2.5.2 (2) In-service pressure tests enable making a safety statement that is comparable to the one made on the basis of the pressure test of the construction process. Pressure tests of the reactor pressure vessel are performed without the reactor core.

2.5.2 (3) Subsequent to the in-service pressure test, a non-destructive test, e.g. with ultrasound, is performed in representative locations of the reactor pressure vessel and other components of the reactor coolant pressure boundary.

2.5.3 Non-destructive in-service inspections

2.5.3 (1) Non-destructive in-service inspections are performed regarding potential damage mechanisms in a representative manner with qualified procedures considering all types of welded joints and base material areas. Selection and suitability of the test procedures and techniques is justified under consideration of the technical progress.

The test intervals are defined. They are oriented towards the general technical experience and consider the operating experiences of the concerned and comparable plants.

2.5.3 (2) Test procedures and techniques are selected such that service-induced flaws (e.g. due to fatigue, corrosion) can be registered and documented with their potential orientations. Indications from manufacturing documented and not removed are registered and monitored as far as required.

2.5.3 (3) Test procedures and techniques for steam generator tubes are selected such that
a) flaws on the inside and outside surfaces, and
b) local wall thinning
will be detected over the entire length.

2.5.3 (4) For each test procedure, evaluation limits are specified for the determination of indications.

3 Pressure-retaining walls of components of external systems

N o t e: For components (vessels, heat exchangers, piping systems, valves, pumps) for which due to the enclosure of the radioactive inventory specific criteria apply which are not assigned to the scope mentioned here, the criteria of the "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components" (Module 10) in Section 5.2 are applicable. Criteria regarding the function of the components mentioned here are also available there.

3.1 Scope

3.1 (1) The following criteria are applied to the pressure-retaining walls of pressure- and activity-retaining systems and components of light-water reactors made of metallic materials that are of safety significance not being part of the reactor coolant pressure boundary. This applies if one of the following criteria is met:
a) For limiting the consequences of an event on levels of defence 3 and 4a, the plant component is necessary with regard to shutdown, maintaining long-term subcriticality and direct heat removal. Criteria for components in systems which only serve to remove residual heat indirectly – these are the non activity-retaining closed cooling water systems and

auxiliary service water systems – are defined plant-specifically under consideration of the general criteria regarding redundancy and diversity; see also “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1 in subsection 3.1 (2)).
b) In case of component failure, large amounts of energy are released and the functions of safety-relevant systems are not protected against impacts of a postulated failure of these components (see “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components“ (Module 10) Section 2.3.6).
c) The failure of the component may lead to an event on level of defence 3 or higher, either directly or in a chain of postulated consequential events.

3.1 (2) The scope of application includes the following components:
a) pressure vessels,
b) piping and piping products (including pressure relief lines and discharge nozzles for BWRs),
c) pumps, and
d) valves,
including the integral parts of the component support structures.

3.1 (3) The scope of application does not include:
a) piping and valves smaller or equal to DN 50. For pipes and valves of this dimensional range, the criteria according to Section 5 apply;
b) component internals (not being part of the pressure-retaining wall) and accessories,
c) plant components performing auxiliary functions for the systems dealt with here,
d) those system parts where the system pressure is solely determined by the geodetic pressure level in the suction region,
e) component parts for force and power transmission
- in pumps and valves, and
- during tests for demonstration of operability,
f) small parts.

3.1 (4) If using components not made of metallic materials, criteria are defined that ensure equivalent reliability.

3.2 Principles of basic safety in connection with design and manufacturing

3.2 (1) The basic safety of the reactor coolant pressure boundary which precludes any catastrophic failure of a plant component as a result of manufacturing defects is ensured by fulfilment of the following criteria under consideration of the operating medium:
- use of high-quality materials, in particular with regard to toughness and corrosion resistance,
- conservative limitation of stresses,
- prevention of stress peaks by optimised design and construction, and
- assurance of the application of optimised manufacturing and testing technologies.

This requires the knowledge and assessment of possibly existing defects.

3.2 (2) Further, the structural layout of all components is such that the criteria for a design not leading to an increase of loads/stresses, meeting the specific requirements for the materials, manufacturing and functions as well as for a maintenance-friendly design are fulfilled and that the non-destructive tests during manufacture and at the place of installation as well as the non-destructive in-service inspections can be performed to a sufficient extent. This applies, in particular, to the welds and the base material of cladded material areas.

3.3 Design

3.3.1 Principles

3.3.1 (1) For ensuring the integrity of the components, an integrity concept is developed which considers the principles presented in this section.

3.3.1 (2) The integrity demonstrations as part of the design are performed such that the required safety distances are shown for all impacts of specified normal operation and from events of levels of defence 3 and 4a over the entire planned lifetime. Potential ageing-induced damage mechanisms and changes of the material properties by impacts such as temperature and irradiation, which may occur during operation, are taken into consideration. The main ageing-induced damage mechanisms are fatigue, relaxation, wear, and different types of corrosion. Moreover, synergisms of different mechanisms are taken into consideration.

3.3.1 (3) The design of components is based on load cases, beginning with impacts. The load cases are derived, in particular, from specified plant operation, from operating experience and from the events postulated according to the “Safety Criteria for Nuclear Power Plants. Events to be Considered in Pressurised and Boiling Water Reactors” (Module 3) and cover the resulting impacts. The load cases and their combinations are specified and completely described according to their characteristics and frequency. Load case combinations are postulated if the events and / or operating phases to be combined may be causally connected or if their simultaneous occurrence has to be postulated according to probability considerations. The impacts resulting from these load cases are described component-specifically also under consideration of the technology of adjacent systems. Impacts from installed components are considered in the integrity demonstration (e.g. with regard to dead weight, support stability, mechanical impacts, thermal-hydraulic conditions) as far as they may influence the integrity of the pressure-retaining walls.

3.3.1 (4) For preventing excess of the pressure permissible on the respective level of defence, reliable systems are provided. The required systems for pressure limitation and overpressure protection can discharge the media to be considered reliably on all levels of defence.

3.3.1 (5) If components of the external systems adjacent to the RCPB are put into operation for the management of events on levels of defence 3 and 4a, the stresses occurring in these systems are limited such that the required reliability of the systems is ensured for the specified lifetime and frequency of use.

3.3.1 (6) For the systems and components addressed within the scope of application, the selection of the materials, manufacturing procedures and verification methods are combined, under consideration of different functional requirements, such that equivalent reliability of the components is reached. Regarding the diversity of components, measures are defined which ensure reliable quality assurance.

This is done for the components by means of classification into test and material groups in dependence of design data and dimensions under consideration of the materials and stress limits. In this respect, different test and material groups may be obtained for components within a system and, potentially, also for parts of a component.

These test groups for parts and components of the external systems also include specifications on verification depth with regard to the scope of the stress and fatigue analyses and to the scope of tests (destructive and non-destructive) in dependence of the stress relative to the permissible stress and material selection.

3.3.2 Material selection

3.3.2 (1) By material selection and adequate structural design, welding and heat treatment, it is ensured for the reactor coolant pressure boundary that throughout the planned lifetime of the plant, a sufficiently strong and tough material condition is maintained such that the loads occurring during specified normal operation and in case of events on levels of defence 3 and 4a can reliably be borne.

For the demonstration of the specified strength and toughness, manufacturing in accordance with the specifications is demonstrated for all materials with certificates. For ferritic steels, a sufficiently high level of upper shelf toughness is given. For loads from stationary operating conditions on levels of defence 1 and 2, the lowest temperature loading exceeds the NDT temperature such that a defined minimum toughness is ensured. This applies to base material, weld material and heat-affected zones.

3.3.2 (2) In combination with the selected construction and the processing techniques applied, the materials used have sufficient resistance against corrosion and other ageing effects under the operating conditions. The water qualities required for corrosion resistance during specified normal operation (levels of defence 1 and 2) are specified. The water quality is monitored and deviations from the specified parameters are detected at an early stage so that disadvantageous impacts on the components are prevented.

3.3.2 (3) The materials, including weld filler materials, to be selected for the respective case of application meet the requirements for the stresses considered in the design and occurring during operation (e.g. mechanical, thermal and chemical stresses). They are generally weldable, have sufficient toughness in accordance with the design concept as specified in Section 3.3.1 and 3.3.4 and show a strong strain hardening behaviour.
N o t e: For ferritic materials, this generally requires the use of low- or medium-strength materials with heat treatment conditions that are common in nuclear technology. Austenitic materials fulfil the last mentioned criteria without any restrictions.

3.3.2 (4) Component parts with sealing a n d / o r sliding function show sufficiently high chemical, mechanical and physical resistance under the conditions given under specified normal operation (levels of defence 1 and 2). Unavoidable corrosion and abrasion products as well as released substances are
– due to their chemical composition
– or due to measures taken

radiologically irrelevant and cause no damage of the components by corrosion.

3.3.3 Construction and arrangement

3.3.3 (1) The components according to Section 3.1 are arranged and installed such that, in case of events on levels of defence 3 and 4a, no consequential damages at other safety-relevant plant components can occur which may endanger the fulfilment of the safety function of these components
N o t e: For the impacts to be considered, see also “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components“ (Module 10, in Section 2 and 2.2.8).

3.3.3 (2) For all components of the pressure-retaining walls of the external systems, adequate possibilities for inspections and in-service inspections are provided. In areas with increased radiation levels, heat insulations at the components to be inspected are designed such that they can fastly be removed and remounted, if required. For better reproducibility of the test parameters and test boundary conditions and for better comparability of the test results as well as for limitation of the radiation exposure of the personnel, mechanisation of the tests is made possible.

3.3.3 (3) Pipes connecting to the isolation devices of the reactor coolant pressure boundary and do not penetrate the containment have an additional isolation device within the containment, as far as no pressure relief into closed containers (e.g. wetwell, relief tank) is provided for reasons of safety.

3.3.3 (4) Components which may be loaded with higher pressure or higher temperature by assumption of a single failure at the isolation device of the adjacent reactor coolant pressure boundary are designed such that their integrity is also ensured in such load cases.

3.3.3 (5) Bolted joints are designed such that the necessary tightness is reached in a reliable manner. Their design is qualified and their suitability demonstrated on the basis of technical experience. They are monitored adequately so that leakages that might occur are detected early enough to prevent impermissible consequences.

3.3.3 (6) Regarding pipes branching off, the isolation valve is located as near as possible to the branch-off point.

3.3.3 (7) Installed components of isolation devices are designed such that they show the necessary load-bearing capacity for ensuring the sealing function.

3.3.3 (8) Pipe laying and spatial arrangement of the valves ensure that accumulations of condensate in steam-carrying plant components are prevented by drainage.

3.3.3 (9) With adequate systems and measures it is ensured that excess of the loads considered in the integrity demonstrations on
a) the main steam line (overfill protection),
b) the components as a result of water hammer,
c) the components as a result of to radiolysis gas reaction,
d) the components of low-pressure systems connecting to high-pressure systems as a result of leaks in isolation devices of the system with higher pressure

are reliably prevented for levels of defence 1 to 3. The effectiveness of the measures is monitored.

3.3.3 (10) With regard to the amounts of exhaust gas, the pressure relief lines and discharge nozzles in BWRs are dimensioned for all events on levels of defence 2 und 3 such that a reliable outflow of the medium (steam, steam/water mixture) into the wetwell is ensured in compliance with the design values.
It is ensured that in the gaseous phase of the wetwell above the water level, no leakages will occur in the pressure relief lines or that leakages that cannot be precluded are reliably discharged (e.g. by installation of a guard pipe).
An accumulation of radiolysis gases in the pressure relief lines due to condensation of potential steam leakages is limited by appropriate measures (e.g. nitrogen purge) such that no reactive mixtures can be produced.
N o t e: Regarding preventive measures, see also “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components“ (Module 10 in Section 2.2.8)

3.3.4 Strength design

3.3.4 (1) The integrity demonstrations give proof on the observance of margins to the occurrence of failure types to be postulated. The stresses caused by mechanical and thermal loads in the components are limited such that for the respective level of defence a safety distance to the occurrence of postulated failure types is given according to the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1). In case of any uncertainties about the state of knowledge on damage mechanisms, these are considered by respective safety margins or conservative safety demonstrations. For the components, preventive measures have been taken against failure due to the following mechanisms:
a) plastic instability,
b) global deformation,
c) ratcheting,
d) fatigue,
e) break due to unstable crack propagation,
f) elastic instability.

3.3.4 (2) The necessary safety distances for the stresses resulting from the loads are defined for the different levels of defence as follows:
a) The stress limits on levels of defence 1 and 2 ensure that the balance between stresses and impacts, including the safety margins specified according to the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1), subsection 3.1 (2), is achieved such that no global plastic deformations, no elastic instability, no break, no failure due to ratcheting and no failure due to fatigue occur. The safety distances are determined such that in case of stresses from internal pressure, weight, fluid dynamics and other, quasistatic impacts, the load-bearing cross sections remain in the range of elastic material behaviour, except for locally limited areas. For additionally acting stationary and dynamic impacts from operating conditions on levels of defence 1 and 2, the safety distances are defined such that, in addition, a failure due to ratcheting and fatigue is not to be postulated.
b) The stress limits on levels of defence 3 and 4a ensure that the balance between stresses and impacts, including the safety margins to be considered (see “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1), subsection 3.1 (2)), is achieved such that a failure due to plastic or elastic instability or due to unstable crack propagation is precluded. The safety distances are selected such that in case of stresses from internal pressure, weight, fluid dynamics and other additional loads from external events being

similar regarding their characteristics, the plastic deformations remain limited. The demonstration for the exclusion of failures due to unstable crack propagation includes, in addition, the impacts from restrained thermal expansion.

c) For events on levels of defence 3 and 4a, plastic deformations are limited to the area of geometric discontinuities. For geometrically simple component parts (e.g. pipes), plastic deformations of the entire cross section are permissible in case of dynamic strains; however, the resulting elongations clearly remain below the uniform elongation of the material, under consideration of the influence of multiaxiality which may lead to a restricted deformability and other effects which may increase the elongations occurring.

   After the occurrence of events on levels of defence 3 and 4a, areas with plastic deformations, identified by calculations, are subjected to a qualified inspection. For the inspection, comprehensible assessment criteria are defined.

3.3.4 (3) For events on levels of defence 3 (e.g. design earthquake) and 4a, whose management requires the function of external systems, the stress limits for the components used for it and other systems used for their function (e.g. supply and cooling systems) are defined such that the operability of these components remains ensured.

3.3.4 (4) The integrity demonstration is performed by experiments or calculations or in combination of these methods. An acceptance target is specified and its fulfilment is demonstrated with validated methods. The applicability of the boundary conditions of the computational methods or experiment to the boundary conditions of the components or systems for which safety demonstrations are required is demonstrated. The observance of the above mentioned safety distance between acceptance target and the failure or occurrence of a state to be prevented is shown.

N o t e: Regarding criteria for experimental verifications and the validation of methods, see also “Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation“ (Module 6).

3.4 Manufacturing

3.4.1 Principles

3.4.1 (1) The quality criteria to be fulfilled for ensuring integrity are defined and considered in the planning of the manufacturing process.

3.4.1 (2) Manufacturing is performed with qualified methods and by qualified manufacturers.

3.4.1 (3) The manufacturing process is monitored and documented such that deviations from specified quality criteria are identified reliably and their causes can clearly be determined. Additional measures taken for achieving the criteria are documented.

3.4.1 (4) For welding materials and supplies, adequate certification tests or qualification tests are performed. The manufacturer verifies by means of corresponding welding procedure qualification tests that he is able to perform proficiently the welding procedures provided.

3.4.1 (5) Weld cladding on ferritic components is designed such that the base material can be subjected to ultrasonic examination methods from at least two surfaces.

3.4.2 Destructive in-process tests

3.4.2 (1) By means of qualified tests on product forms it is demonstrated that the specified properties of chemical composition, toughness, structural strength and corrosion resistance are present across the wall thickness.

3.4.2 (2) The mechanical-technological properties generally are demonstrated for each product form (component-wise or batch-wise) which includes the following:

a) representatively, the different deformation directions at several sampling points, and
b) all transformation and heat treatments taking place during the manufacturing process.

3.4.2 (3) For verification of the quality characteristics of production welds, production weld tests are performed. It is permissible to combine the performance of production weld tests with welding procedure qualification tests.

3.4.2 (4) For weld-cladded product forms, proof is given that there are no underclad cracks. In justified cases, this may also be done by non-destructive tests on the components.

3.4.3 Non-destructive in-process tests

3.4.3 (1) For all product forms and welds, including butterings, provided for the pressure-retaining walls, the volume and surfaces are subjected to non-destructive tests with sufficient detectability of discontinuities. Weld claddings are tested for adhesion and fault-free condition of the surface.

The techniques and parameters for the volumetric examination are selected such that all safety-relevant flaws are detected. This requires that the examinations are performed with sensitivities which allow detection of indications with dimensions clearly below the size of safety-relevant flaws. In this respect, flaws oriented perpendicular to the principal stress directions (operating stresses) are considered by selecting qualified techniques and parameters (such as sound propagation directions).

The permissible limits for indications in the volume are generally defined such that technically relevant changes of the indication dimension by impacts from operation are not to be expected.

The surface tests cover all flaw orientations of the test geometry. Crack-like indications at the surface are not permissible. Methods for removal of surface crack indications are qualified regarding the damage mechanisms to be considered during operation. Application according to the specification is monitored and confirmed by tests.

3.4.3 (2) Type, timing and scope of the non-destructive tests are defined depending on the product form and component in accordance with the classification into test and material groups according to subsection 3.3.1 (6). The test for assessment of the relevant quality conditions of the product forms and components is performed after the last heat treatment.

3.4.3 (3) At the end of the manufacturing process, all pressure-retaining components of the external systems are subjected to a pressure test defined above the design pressure (initial pressure test). After the pressure test, non-destructive tests are performed within a representative scope.

3.5 Operation

3.5.1 Principles

3.5.1 (1) For maintenance of the barrier function, a monitoring and testing concept is established for

- checking compliance with the design boundary conditions and prerequisites, and
- ensuring operating experience feedback and its use in ageing management.

The boundary conditions regarding spatial layout, anchoring, function of supports, valves, pumps and internals on which the design of the components and systems is based are documented (e.g. free path lengths, displacements, deflections, clearances for high-temperature systems). During commissioning and, as far as required, after interferences (e.g. maintenance measures), compliance with the boundary conditions is checked. Impermissible deviations from these boundary conditions are prevented or identified in sufficient time such that no impacts on the integrity of the pressure-retaining walls take place.

3.5.1 (2) Operating parameters which are significant for the integrity of the components (e.g. mechanical and thermal loads, water quality) are monitored and checked for plausibility under consideration of the respective postulated system state. Moreover, monitoring for leaks is provided which ensures the detection and sufficiently precise localisation of leakages.

3.5.1 (3) The operating conditions in the operating phases of low-power and shutdown operation (operating phases B - F) and during functional tests are specified with regard to the impacts influencing the integrity of components. The fulfilment of these requirements is ensured by the operating instructions (e.g. temperature, water chemistry). Deviations from these specifications are prevented or identified in sufficient time such that no impacts on the integrity of the pressure-retaining walls take place.

3.5.1 (4) Components or component areas for which relevant stresses are to be expected according to analyses or due to operating experience with regard to ageing-induced damage mechanisms are included in a monitoring and testing concept.

3.5.1 (5) The general condition of the systems and components is monitored by regular walk-down. The results are documented.

3.5.1 (6) It is ensured that on levels of defence 1 and 2 the amounts of hydrogen (radiolysis gases, added hydrogen) which can permeate from the circuits into a non-inerted atmosphere of the containment remain limited such that an explosive accumulation with potential for consequential damage can be precluded.
N o t e: See also “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components“ (Module 10 in Section 2.2.8.2).

3.5.1 (7) Accumulations of non-condensable gases
a) at the highest point of the cooling circuit,
b) in components with no or only small through-flow
are recorded with regard to potential thermal impacts on the pressure-retaining wall and potential malfunctions of the system. They are assessed with regard to their safety-related consequences.

3.5.1 (8) If relevant indications are identified during the examinations, proceeding shall take place according to Section 8.

3.5.1 (9) For systematic identification, surveillance or prevention of ageing impacts on the integrity of the pressure-retaining walls of components, an ageing management system is implemented.

3.5.1 (10) The technical systems and auxiliary equipment as well as the handling procedures employed for work on the pressure-retaining components of the external systems (e.g. on threaded joints during tests and cleaning) are qualified such that detrimental impacts on the components are prevented or identified in sufficient time such that no impermissible impacts on the integrity of the pressure-retaining walls take place.

3.5.1 (11) The testing concept is updated with regard to the remaining operating life well before the end of operation. Planned tests are scheduled such that there will be a gain in safety.

3.5.2 In-service leak and pressure tests

3.5.2 (1) After each reclosure of a pressure-retaining system, an integral leak test is performed under a defined reference condition.

3.5.2 (2) In-service pressure tests enable making a safety statement that is comparable to the one made on the basis of the pressure test of the construction process.

3.5.2 (3) Subsequent to the in-service pressure test, a non-destructive test, e.g. with ultrasound, is performed on representative locations of the pressure-retaining walls of the different components.

3.5.3 Non-destructive in-service inspections

3.5.3 (1) Non-destructive in-service inspections are performed regarding potential damage mechanisms in a representative manner with qualified procedures considering all types of welded joints and base material areas. Selection and suitability of the test procedures and techniques is justified under consideration of the technical progress.

The test intervals are defined. They are oriented towards the general technical experience and consider the operating experiences of the concerned and comparable plants.

3.5.3 (2) Test procedures and techniques are selected such that service-induced flaws (e.g. due to fatigue, corrosion) can be registered and documented with their potential orientations . Indications from manufacturing documented and not removed are registered and monitored as far as required.

3.5.3 (3) For each test procedure, evaluation limits are specified for the determination of indications.

4 Additional criteria for components and systems for the limitation of break assumptions

4.1 Principles

4.1 (1) If limited leak and break assumptions are made use of within the framework of the design concept for piping systems and components of the reactor coolant pressure boundary according to Section 2.1 or the external systems according to Section 3.1 as specified in Annex 2 of the “Safety Criteria for Nuclear Power Plants: Events to be Considered in Pressurised and Boiling Water Reactors“ (Module 3), these are to be protected against external events from events of level of defence 4a by structural measures or decoupling and, under consideration of the vibrations induced by these events, designed such that their integrity is maintained. Moreover, in addition to the criteria according to Section 2 and 3, an analysis is performed which comprises any potential loads resulting from levels of defence 1 to 3, under consideration of the response behaviour of the system. With enveloping impact assumptions derived from it, it is demonstrated under the assumption of defects that these defects cannot lead to a leak or break of the components which put the leak and break assumptions made use of into question. The defects are selected such that they develop more unfavourable under the resulting loads regarding the integrity of the components than defects that may be existing in the component and that are reliably identifiable.

4.1 (2) The size of the defects to be postulated is determined such that they can be identified reliably with the specified test procedures. The defects are postulated at that surface and in the orientation for which the largest growth potential is given.
N o t e: Specific assumptions and approaches for different component groups are stated in the following subsections of Section 4.

4.1 (3) The criteria according to Section 2 and 3 for the components concerned are fulfilled. This ensures the prerequisites for using limited leak and break assumptions, i.e.

- damage mechanisms such as corrosion and erosion processes, fatigue caused by vibrations and dynamic loads as well as operational material changes are limited and identifiable such that they cannot lead to any relevant damage,
- stress limitation is not endangered by overpressure, additional thermal and mechanical loads or malfunctions of the supports.

4.2 Break preclusion demonstration for the reactor pressure vessel

4.2 (1) For the reactor pressure vessel, whose integrity is necessary in ensuring the achievement of all protection goals according to the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1), all changes of the material properties to be expected during the planned lifetime are conservatively considered for the demonstration of break preclusion.

4.2 (2) For areas of the RPV wall exposed to neutron radiation, the fluences are limited by structural requirements and requirements for a chemical composition fulfilled in the base material and the weld metal so that the changes of strength and toughness properties due to radiation remain within permissible limits.

4.2 (3) For the characterisation of material properties changed by radiation, a surveillance programme adapted to the accumulated neutron fluence is performed with accelerated irradiation specimen capsules (base materials, welded joints).

4.2 (4) For postulated surface defects and manufacturing defect sizes in the volume which might be identified, it is verified for all stresses from the relevant loads that, when using fracture-mechanical methods for verification,

- no crack initiation occurs during operating conditions of levels of defence 1 and 2, and
- no unstable crack growth takes place in wall thickness direction in case of events on levels of defence 3 and 4a.

For events on levels of defence 3 and 4a, a limited stable crack growth, not significant regarding the wall thickness, is only permissible in the upper shelf of toughness.

Moreover, it is demonstrated by calculations that crack growth of the defect sizes considered under cyclic loading is not significant with regard to the wall thickness.

4.3 Break preclusion for pipes

If the break preclusion approach is applied to the piping systems according to Section 4.1, it is demonstrated:

- that postulated defects in the pressure-retaining wall show no significant growth regarding the wall thickness in case of operating conditions and events to be postulated on levels of defence 1 and 2,
- a postulated through-wall crack at the pressure-retaining wall resulting from events on level of defence 3 remains stable, i.e. leak-before-break behaviour is shown. It is demonstrated that, under consideration of the loads resulting from the leak case and the grace times for detection of the leak until shut down of the system affected, a sufficient margin to critical crack sizes is maintained. The size of the postulated crack is determined such that detection of the leak caused by these cracks during operation is ensured in due time. Leak detection is performed with a high degree of reliability and ensured by the use of diverse measuring methods.

4.4 Break preclusion demonstration for vessels

If the break preclusion approach is applied to vessels according to Section 4.1, it is demonstrated that no unstable crack growth takes place in wall thickness direction in case of operating conditions and events on levels of defence 1 to 4a. A limited, stable crack growth is only permissible in the upper shelf of toughness, maintaining a sufficient margin to critical crack sizes.

4.5 Break preclusion demonstration for housings

If the break preclusion approach is applied to valve housings according to Section 4.1, it is demonstrated that no unstable crack growth takes place in wall thickness direction in case of operating conditions and events on levels of defence 1 to 4a. A limited, stable crack growth is only permissible in the upper shelf of toughness, maintaining a sufficient margin to critical crack sizes.

4.6 Preventive measures for demonstration of leakproofness

For sections of high-energy piping systems of the reactor coolant pressure boundary and the external systems between the containment and the external isolation device which in case of a leak might lead to

- impermissible pressure build-up in the surrounding building, or
- impermissible impacts on safety-relevant installations (e.g. flooding, jet forces, temperature, humidity), or
- an impermissible release of reactor coolant outside the building

for which, however, no consequential damages from leaks at them are considered in the safety demonstration, break preclusion is demonstrated according to Section 4.3.

Moreover, the following is applicable:
– The constructive criteria of basic safety for prevention of stress peaks are implemented in an optimal manner.
– The spatial extension of the areas concerned is very limited.
– They do not have branch pipes or welding areas.
– For the validation of the integrity demonstration, they are monitored such that locally occurring impacts are known,
– For the connecting containment (PWR) and steam line (BWR) isolation valves, break preclusion is demonstrated according to Section 4.5.

5 Small-diameter pipes

5.1 Scope

The following criteria are applied to the pressure-retaining walls of pipes and valves with nominal diameters smaller than or equal to DN 50 which are assigned regarding systems technology to the reactor coolant pressure boundary or the external systems.

5.2 Design

5.2 (1) There are provisions laid down in written which
– comprehensively cover potential impacts on piping systems and valves,
– cover the layout geometries realised, and
– define specifications for pipe supports under consideration of load transfer.

5.2 (2) Dimensioning, laying and support of the pipes and valves comply with these written specifications and are documented. These specifications ensure that
– for the operating conditions and events of levels of defence 1 to 3, the service limits of the external systems according to subsection 3.3.4 (2) of the respective test and material group (see in subsection 3.3.1 (6) are complied with.
  By specific provisions on the integrity of the piping systems under dynamic excitations, in particular from the connecting systems and components, single failure is prevented and systematic failure (e.g. due to fatigue, rupture, buckling) precluded.
– impacts from events of level of defence 4a do not lead to a failure which puts the effectiveness of the measures and systems required for the control of the respective event in question.

5.2 (3) The piping systems and valves are arranged and installed or potentially affected plant components protected such that in case of postulated failure of a pipe no consequential at other safety-relevant plant components can occur which may endanger the fulfilment of the safety function of these components.

5.3 Material selection and manufacturing

5.3 (1) Material selection and manufacturing quality ensure that under consideration of the operating media and conditions specific damage mechanisms do not lead to systematic failure.

5.3 (2) At the end of the manufacturing process, the pressure-retaining walls of pipes and valves are subjected to a pressure test at a test pressure higher than the design pressure (initial pressure test).

5.4 Operation

During commissioning, as far as required after interferences (e.g. maintenance measures) and within a representative scope, laying, position and function of supports is checked by in-service inspections, also including leakage tests. For the determination of the representative scope, the safety significance is taken into consideration. Impermissible deviations from documented boundary conditions are detected early enough to prevent systematic impacts on the integrity of the pressure-retaining walls during long-term operation and thus the required reliability for failure free operation is given.

6 Guard pipes (double pipes)

For sections of piping systems with media that are carried in a guard pipe to prevent impermissible consequential effects from the leaks and breaks to be postulated at them, the following criteria are fulfilled:
- The guard pipe is designed such that the impacts from the leaks and breaks of the medium-carrying pipes are transferred without global plastic deformation.
- The design of guard pipes, which assume the function of the containment in case of demand, corresponds at least with the design conditions of the containment.

7 Containment system

7.1 Scope

The containment system comprises the following components:

a) Containment made of reinforced and prestressed concrete with steel lining, including
- personnel locks,
- material lock,
- pipe penetrations,
- isolation system,
- cable penetrations,
- pressure suppression system for BWRs (including the associated components for injection of the released reactor coolant into a water pool),

b) surrounding building,
c) auxiliary systems for retention and filtering of potential leakages from the containment,
d) auxiliary system for prevention of impermissible local and global accumulation of hydrogen in the containment atmosphere,
e) systems for pressure limitation in the containment.

N o t e: The criteria for the following components of the above listing are not all dealt with in full. Criteria for the surrounding building are only dealt with regarding their function for the containment system. Further criteria are to be found for:
- auxiliary systems for retention and filtering in “Safety Criteria for Nuclear Power Plants: Criteria for Radiation Protection“ (Module 9)
- auxiliary systems for hydrogen reduction in “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components“ (Module 10)
- accident management measures in “Safety Criteria for Nuclear Power Plants: Criteria for Accident Management“ (Module 7).

7.2 General criteria for the containment system

7.2 (1) The containment system fulfils the retention function such that the release of radioactive materials into the environment is kept as low as possible and the limits specified for levels of defence 1 to 3 are not exceeded. The leak-tightness requirements for the containment required for it are quantified by a maximum permissible leak rate for the operating phases in which the containment is closed.

The maximum permissible leak rate of the containment in case of events on level of defence 3 is determined on the basis of the accident analysis of the plant and the radiological safety goals stipulated in the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1, in Section 2.4).

7.2 (2) The containment is surrounded by a building. The building is designed such that the space between containment and building can be kept at sufficient negative pressure in the long term during operating phases with closed locks even in case of conditions of events on level of defence 3 in the containment. For this purpose, there are structural provisions for the surrounding building which ensure air tightness. The interspace is vented via stack and, if required, via filters. Further, it allows inspection of safety-relevant plant components.

Further, there are structural provisions which ensure tightness of the building against precipitation water during the entire operating life of the plant.

7.2 (3) The surrounding building shields the outside from direct radiation to a sufficient degree and protects the containment and its internals against impermissible consequences from the external events considered for the plant.

7.3 Containment design

7.3 1 Principles

7.3.1 (1) The containment including all penetrations and locks as well as the pressure suppression system for pressure limitation in boiling water reactors are designed such that, under consideration of the allowed leakage rate, they withstand the static, dynamic and thermal loads (e.g. forces, internal and external overpressure and temperatures, pressure differences, missiles and jet forces) from operating conditions and events on levels of defence 1 to 3 as well as from anticipated transients without scram on level of defence 4a.

Further, systems are provided for preventing a failure of the containment due to overpressure or impermissible dynamic loads from hydrogen reactions also in case of postulated event sequences and plant conditions on levels of defence 4b and 4c.

7.3.1 (2) Regarding the containment venting required for the prevention of failure due to overpressure see “Safety Criteria for Nuclear Power Plants: Criteria for Accident Management“ (Module 7, in subsections 3.1 (2) and 4.2 (3)).

7.3.1 (3) The containment including its isolation valves, locks, penetrations and the pressure suppression system for pressure limitation in boiling water reactors as wells as the internals required for its function are protected against consequential impacts from events on level of defence 3 (missiles, jet and reaction forces) and from anticipated transients without scram on level of defence 4a by structural provisions (missile shield) such that their operability is maintained. Further the containment is protected by structural decoupling such that its support stability is also maintained in case of man-made hazard conditions of level of defence 4a. Likewise, the support stability or integrity of internals and rooms, including, as far as necessary, the effect of pressure differences, is maintained in case of all events of levels of defence 3 and 4a. This applies to the prevention of impacts on the containment emanating from the internals and on the maintenance of all necessary functions of the internals, such as support function for components, flow control, and physical separation.
N o t e: Specifications for the determination of the differential pressures are included in the “Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation“ (Module 6), Annex 2.

Specifications for the determination of impacts from jet and reaction forces as well as missiles are included in the “Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation“ (Module 6), Annex 3.

7.3.1 (4) For ensuring an appropriate pressure differential, the containment penetrations are sufficiently tight during specified normal operation of the operating phases A und B and events on level of defence 3.

7.3.2 Construction and arrangement

7.3.2 (1) The design of the containment includes equipment for the performance of pressure and leak rate tests and for the installation of the instrumentation necessary for it.

7.3.2 (2) Locks and dampers required for the containment system are connected to a leak-off system by which the leakages can be pumped back into the containment.

7.3.2 (3) The penetration chambers are testable at design pressure of the containment.

7.3.2 (4) Safe handling of the hydrogen (radiolysis gases, added hydrogen) within the containment is ensured during specified normal operation (levels of defence 1 and 2) and in case of any loss-of-coolant accidents (level of defence 3).
N o t e: See also “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components” (Module 10, in Section 2.2.8).

7.3.2 (5) Locks are provided for introducing and removing materials and objects into or out of the containment as well as for entry and exit of persons.

Material locks serve exclusively for the purpose of transferring materials or objects.

Personnel locks are positioned such that an escape from the containment is possible as fast as possible with the lowest possible radiation exposure of persons. In this respect, it is considered, in addition to radiation fields and contaminations, that escape routes may be blocked, e.g. by escaping media like water, steam or gases.

It is ensured by interlocks that in the operating phases in which the locks shall be closed a hatch can only be opened when the other hatch is shut and after the pressure equalisation device of the latter is closed and sealed. Disengagement of the interlock is only permissible under conditions permissible from the safety point of view.

7.3.2 (6) The number of penetrations is as small as practically feasible. In order to avoid retrofitting with nozzles, spare nozzles and spare ducts are provided.

7.3.2 (7) The cross sections of the lines necessary for ventilation of the containment are kept as small as possible.

7.3.2 (8) For transitions between concrete and steel containment shell and the elastic seals, qualified designs are provided.

7.3.2 (9) As far as occurrence of impermissible negative pressure due to events of levels on defence 2 to 4a cannot be excluded, there are reliable systems and devices for the prevention of negative pressure.

7.3.2 (10) Pipes that are in contact with the reactor coolant or the internal atmosphere of the containment and penetrate the latter generally have two isolation valves, one of them located within the containment and the other outside as near as possible to the containment. Exceptions are permissible if these are necessary due to the technical features or operating mode (e.g. valves that have to be opened for accident management) of the pipe concerned and if the safety function of the containment system is not impaired.

Pipes that penetrate the containment but are not in contact with the reactor coolant or the internal atmosphere of the containment are equipped at least with one isolation valve outside the containment.

7.3.2 (11) All penetrations through the containment wall and the locks in the containment at least fulfil the design criteria for the containment.

This also applies to pipes penetrating the containment wall up to the external isolation device, the associated containment isolation devices and, where applicable, the penetration chambers.

For ventilation ducts, this also applies to the duct section between the isolation valves and the associated isolation devices themselves.

7.3.2 (12) The spatial layout of the penetrations fulfils the requirement for separation of redundant systems which results from the conceptual design of the entire plant. Damage at a penetration, including breaks of connecting pipes, if any, does not lead to an consequential damage at other penetrations.

7.3.2 (13) Penetrations which have to be closed to maintain the function of the containment are secured by a redundant design of successively installed containment isolation valves. Each containment isolation valve as such fully complies with the specified tightness conditions.

7.3.2 (14) Systems for prevention of overpressure between the isolations are provided, as far as necessary.

7.3.2 (15) For sections of high-energy piping systems of the reactor coolant pressure boundary and the external systems between the containment and the external isolation device which in case of a leak might lead to

- impermissible pressure build-up in the surrounding building, or
- impermissible impacts on safety-relevant installations (e.g. flooding, jet forces, temperature, humidity), or
- an impermissible release of reactor coolant outside the building,

additional demonstrations and criteria for the use of limited break assumptions according to Section 4.6 are made and fulfilled so that consequential damages from leaks at them do not have to be postulated.

N o t e: See also “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components” (Module 10, in Section 4.2.4).

7.3.2 (16) The penetration is designed such that it has sufficient load-bearing capacity for all forces and moments of the penetrating pipe during specified normal operation and events on levels of defence 3 and 4a. Penetrations which cannot rigidly be connected to the containment nozzles due to high loadings are connected with expansion joints and chambered.

7.3.2 (17) The closure speed of the containment isolation valves ensures that no impermissible impacts occur.

7.3.2 (18) Short pipe lengths are preferably used between the isolation valves and the containment. In such areas, pipe branching is basically not permitted. Exceptions (such as drain nozzles, test assemblies) are subjected to a safety analysis.

7.3.2 (19) For pipes penetrating the containment, the structures within the containment are decoupled from mechanical impacts due to events of levels of defence 2 to 4a outside the containment by appropriate constructions such that consequential failure within the containment is not to be postulated.

7.3.3 Strength design

7.3.3 (1) For ensuring integrity and specified tightness, the maximum pressures and temperatures occurring and loading due to events on level of defence 3 are determined. In this respect, margins are to be considered for

a) uncertainties of the release rates of mass and energy, including chemical energy from metal reactions,
b) tolerances in the building and structure modelling,
c) uncertainties regarding the decay heat generation,
d) the non-consideration of the thermodynamic disequilibrium between gas and liquid phase, and
e) the selection of a corresponding correlation for the heat transition are considered.

An adequate safety margin to the maximum overpressure resulting from it is considered for

- model uncertainties and
- the most unfavourable initial operating conditions

when determining the design pressure.

7.3.3 (2) The containment of a PWR is designed such that the load-bearing capacity is sufficient for the mass and energy content of the reactor coolant pressure boundary and the secondary side of a steam generator up to the secondary-side isolation. In addition, the heat transfer of the steam generators to the escaping reactor coolant has been taken into consideration.

7.3.3 (3) The containment of a BWR with pressure suppression system is designed such that the load-bearing capacity is sufficient for the mass and energy content of the reactor coolant pressure up to the reactor-side isolation. The loads resulting from incidents and their impacts, such as pressure build-up, pressure relief and suppression processes and vibrations produced as well as simultaneous occurrence of such processes are considered for the impact on the containment, the pressure suppression system and other systems with their maximum effects.

The design also considers those amounts of water and steam which may flow back into the containment or may be injected through the main steam or feedwater lines during closure of the valve. Atmosphere and water level in the wetwell are considered with separate energy balances (disequilibrium). The condensation effect of the water pool is considered regarding pressure suppression.

The anchors and supports of the safety relief valves, pressure relief lines and vent pipes necessary in a BWR in the area of the wetwell of the containment are designed such that they bear the loads from operating conditions and events on levels of defence 1 to 3 as well as from anticipated transients without scram on level of defence 4a (fluid dynamic loads, jet and reaction forces) in a reliable manner. Moreover, structural or procedural systems and measures are available so that the integrity of the containment structure is not impaired by jet and impulse forces of the vent pipes.

7.3.3 (4) For ensuring support stability and integrity, in particular with regard to the tightness of the containment and its components, an integrity concept is applied which considers the following principles:

a) The load cases and their combinations to be assigned to the respective level of defence are clearly specified (e.g. in a load case catalogue including type, extent, frequency and time distribution of the loads). With regard to load combinations, load contributions which may be effective simultaneously are superposed.
b) The loads resulting from these load cases are described component-specifically (e.g. in design data sheets).
c) The stresses resulting from the loads are limited such that for each level of defence a sufficient safety distance to the failure types to be anticipated is ensured.

7.3.3 (5) Measures and systems are provided for a steel containment and its components according to Section 7.1 against the following types of failure:

a) elastic and plastic buckling,
b) global deformation,
c) local deformation and ratcheting,
d) fatigue.

The safety distances maintained in this respect for the stresses resulting from the loads are, according to the levels of defence, specified as follows:

– The stress limits for operating conditions and events on levels of defence 1 to 3 and anticipated transients without scram on level of defence 4a ensure that the tightness function is maintained.
– The safety distances are selected such that for all static and dynamic loads, elastic or plastic buckling does not occur and that for all static loads, the load-bearing cross sections remain in the range of elastic material behaviour. In case of time-dependent loads (specified load collective), the safety distances are defined such that a failure due to fatigue is not to be postulated.
– For one-time local stresses (e.g. during pressure tests), the safety distances are determined such that plastic deformations remain limited to partial areas of the cross section. The extent of permissible plastic deformations is defined in dependence of the component and the material.

For ensuring the tightness function in case of demand, form stability and, as far as applicable, deformation limitation is verified.

7.3.3 (6) The following criteria are fulfilled for a containment made of reinforced and prestressed concrete:

a) For ensuring tightness, steel lining is provided which is anchored in the concrete support structure such that its tightness function is maintained under all loadings from operating conditions and events on levels of defence 1 to 3 and anticipated transients without scram on level of defence 4a. Penetration liners and pressure-retaining steel parts of the penetrations are designed and anchored such that they have sufficient load-bearing capacity for forces from pressure and temperature impacts, piping reactions and other loads occurring during events on levels of defence 1 to 3 and anticipated transients without scram on level of defence 4a.

b) For events of level of defence 3 and anticipated transients without scram on level of defence 4a, local damage or cracking of the concrete is permissible. However, the load-carrying capacity of the overall construction is maintained and the safety function is fulfilled according to the criteria of the respective level of defence.
c) For reinforced and prestressed concrete structures, it is verified under internal pressure for the planned lifetime of the plant during normal operation and for events on level of defence 2 that the prestressed concrete shows quasi-elastic behaviour. Here, locally limited inelastic behaviour is permissible. Support stability of the concrete support structure and tightness of the liner are verified.
d) During the entire planned plant life, the contraction and relaxation processes occurring are considered such that the integrity and tightness of the liner and the transition areas is maintained under these processes and the loads from events on level of defence 3 and anticipated transients without scram on level of defence 4a. Maintenance of the function of safe enclosure of the radioactive material is demonstrated.

7.4 Material selection and manufacturing of the containment

7.4.1 Principles

7.4.1 (1) Quality criteria are defined and fulfilled during planning of the manufacturing process which ensure the integrity of the containment.

7.4.1 (2) The manufacturer has qualified manufacturing and test equipment which allow manufacturing and appropriate processing according to the specified requirements under consideration of the requirements for materials and components.

7.4.1 (3) The manufacturing process is monitored and documented such that deviations from specified quality criteria are identified reliably and their causes can clearly be determined. Additional measures taken for achieving the criteria are documented.

7.4.1 (4) For welding materials and supplies, adequate certification tests or qualification tests are performed. The manufacturer demonstrates by means of corresponding welding procedure qualification tests that he is able to perform the intended welding procedures proficiently.

7.4.1 (5) For the fresh concrete delivered, the conformity criteria according to the standards are fulfilled.

7.4.1 (6) Regarding the prestressed steel and the prestressing system, prestressed steel and an appropriate prestressing system, approved according to the applicable standards, is used for the intended purpose or approval is performed in the individual case.

7.4.1 (7) The joining procedures provided for manufacturing are qualified such that the specified tightness can be reached under stresses on levels of defence 1 to 3 and anticipated transients without scram on level of defence 4a in a reliable manner.

7.4.1 (8) Moreover, steel containments fulfil the following criteria:

a) Construction and surface condition of the containment allow sufficient non-destructive testing with informative results, in particular of the welds. Areas no longer accessible for in-service inspection at appropriate intervals due to the structural plant design are designed such that corrosive influences are prevented.
b) The materials, including weld filler materials, load-bearing nuts and bolts, are selected such that they meet the functional requirements (tightness) and the requirements for the stresses to be postulated (e.g. mechanical, thermal and chemical stresses). The material properties, the joining procedures provided and the quality assurance measures are defined such that quality and examinability is reached that meets the requirements in a reliable manner.
   N o t e: For the steel shell, medium-strength, weldable fine-grained structural steels shall preferably be used.
c) The material properties ensure that a sufficiently tough material condition is maintained under all operating- and incident-induced plant conditions.

7.4.2 Destructive in-process tests

7.4.2 (1) By means of qualified tests on product forms, it is demonstrated that the specified properties of toughness, strain, strength and microstructure are present across the wall thickness.

7.4.2 (2) The specifications on the type and scope of tests to be performed, described in the relevant rules and regulations, are adhered to; as far as they do not include any specifications, these are stated separately. In addition to these tests, the mechanical-technological properties are demonstrated for each product form (component-wise) which includes the following:
a) representatively, the different deformation directions at several sampling points, and
b) all heat treatments taking place during the manufacturing process.

7.4.2 (3) For verification of the quality characteristics of production welds, production weld tests are performed. It is permissible to combine the performance of production weld tests with welding procedure qualification tests.

7.4.3 Non-destructive in-process tests, pressure and leak rate tests

7.4.3 (1) The product forms and welds are subjected to non-destructive tests with sufficient detectability of discontinuities (e.g. ultrasonic examination, radiographic examination, surface test). The test techniques and orientations for the welds are selected such that all safety-relevant flaws parallel and perpendicular to the welds are detected. This requires that the examinations are performed with sensitivities which allow detection of indications with dimensions clearly below the size of safety-relevant flaws. Component surfaces are examined from both sides. Crack indications at the surfaces are removed.

7.4.3 (2) Prior to commissioning, the containment, its penetrations and their chambers are subjected to a pressure test for integrity demonstration. Containments for which negative pressure is provided or may occur as operating case are tested accordingly.

This pressure test is monitored by in-process stress and strain measurements for the detection of potential deviations from the specifications. After the pressure test, representative non-destructive tests are performed.

7.4.3 (3) The tightness of the containment is verified by an integral leak rate test.

7.4.3 (4) The initial leak rate test is performed, beginning with unpressurised condition of the containment with gradual pressure increase, at overpressure and at the design pressure provided for in-service leak rate tests.

The in-service leak rate tests, performed at regular intervals, are performed at such pressures where the measured leak rates are reproducible and where conclusions can be drawn on the leak rate at design conditions to a sufficient extent.

7.4.3 (5) As a matter of principle, all penetrations of the containment as far as the first inner or outer anchor as well as their first internal or external isolation devices are already in place at the time of the first integral leak rate test. The containment penetrations are closed by the corresponding isolation devices, actuated by their operational drives. During the test, blind closures may be used on those systems which will not have any direct contact with the containment atmosphere during later operation.

7.5 Operation of the containment

7.5.1 Principles

7.5.1 (1) Operating data relevant for the function of the containment are monitored. For full-pressure containments, this concerns the maintenance of negative pressure. For containments with a pressure suppression system, the effectiveness of separation between drywell and wetwell is included in the monitoring, in addition to the maintenance of negative pressure. For prestressed steel containments, appropriate measures are defined for evaluating the prestress retention. As far as inertisation or partial inertisation is provided, the effectiveness of inertisation is also monitored. Measurements provided to show functional impairment of the containment are either performed redundantly or signals from diverse systems are used.

7.5.1 (2) For the use of seals and seal components made of materials which may lose their effectiveness due to the ambient conditions, the loadings or loading frequency, maximum service lives are defined. The replacement of seals is monitored according to the specifications.

7.5.1 (3) For work processes in the containment, cleanliness conditions are defined. In particular, the entry of corrosive products into areas of the containment which are not accessible for regular tests is prevented.

7.5.2 Non-destructive in-service inspections, leak rate and leakage tests

7.5.2 (1) In order to ensure the required tightness of the containment throughout the planned lifetime of the plant, in-service inspections of the integral leak rate are performed at regular intervals.

7.5.2 (2) The first in-service leak rate test for the containment is performed prior to first power operation. All following in-service inspections at appropriate intervals of the integral leak rate are performed at the end of each outage after completion of all maintenance and repair work which may change the tightness of the containment.

7.5.2 (3) The tightness of the components connected to the leak-off system and the system as such are determined quantitatively at the beginning and at the end of each inspection outage.

7.5.2 (4) The reliability of the containment isolation including the required tightness is determined for the conditions prevailing during a loss-of-coolant accident with the highest pressure build-up in the containment.

7.5.2 (5) Operability, tightness and actuation speed of valves for isolation of the containment are checked regularly.

7.5.2 (6) The pipe penetration chambers of the containment, the locks, cable penetrations and access panel are checked for tightness regularly and after maintenance measures during operation.

7.5.2 (7) Mounting apertures and reserve penetrations are checked for tightness after use.

7.5.2 (8) In BWRs with pressure suppression system, the permissible leak rate between drywell and wetwell is defined and verified by measurements prior to tightness tests.

7.5.2 (9) The components of the containment system are regularly inspected at representative locations, e.g. regarding mechanical and corrosive damage. In particular, the transitions between steel shell and concrete and the elastic seals are covered by these inspections.

8 Handling of indications on components and pipes

8 (1) The following criteria are applicable to components and piping systems of the RCPB and the external systems but not to heat exchanger tubes.

8 (2) Findings are made during in-service or event-related tests. If an assessment limit is exceeded, this is termed as indication. If for the areas subjected to the tests results are available from previous tests, these are referred to for comparison. The comparison is made under consideration of the quality and informational value of the test methods and the respective evaluation methods referred to. The test results are evaluated on the basis of the steps performed and documented with regard to all relevant test parameters.

If a an indication assessed this way occurs for the first time or if a change during operation cannot be precluded according to the comparison with the results of previous tests, additional measurements are performed to determine the type, location and size of the indication. With regard to the acceptance target, a type of failure and a corresponding dimensioning is assigned to the indication determined this way in a conservative manner. The cause of the type of failure is determined and the damage mechanism is stated. In this respect, the possibility of a systematic failure cause is also considered in particular. Where required, additional methods are applied to determine the cause.

In a further analysis it is shown

- to what extent the fulfilment of the requirements on the design was affected by the failure, and
- what possibilities are available for prevention of the causes in future.

Control checks are performed on comparable components or component areas where the damage cause identified or postulated might also occur to clarify whether there is a systematic failure cause.

8 (3) Failures identified that may impair the fulfilment of the requirements of the design concept under the specified impacts of levels of defence 1 to 4a are not left as they are. Failures identified for which an operation-related cause cannot be excluded, are generally not left as they are.

In justified exceptional cases of leaving failures as they are, the failures are assessed with appropriate methods so that a potential further development of the failure is determined conservatively for the specified operating time. Under these prerequisites it is demonstrated that impermissible effects on safety can be excluded under consideration of all impacts of levels of defence 1 to 4a. Control checks are provided for verification of the predicted failure development. Scope and timing are determined according to the safety significance.

Further, it is demonstrated that

- failures left as they are in this way are not related to a systematic cause which may lead to other failures, thus requiring numerous monitoring and control measures
- there is no accumulation of failures, which can lead to an impermissible safety-relevant impairment of integrity of the component affected or reliability of the systems affected when considering each failure separately or by way of interaction.

8 (4) It is checked whether the type and size, circumstance and time of detection or occurrence frequency of failures suggest any gaps or deficiencies in the system- and component-specific requirements (e.g. specifications, testing manual). If required, respective gaps are closed and deficiencies removed. New insights resulting from the cause analysis are integrated into the technical documentation (e. g. with regard to the specified impacts, water chemistry, vibrations) und considered within the ageing management. As far as required, corresponding measures are also taken on the components concerned or regarding their operating mode.

E

MODULE 5
"Criteria for Nuclear Power Plants: Criteria for Instrumentation and Control and Accident Instrumentation"

Contents

1 Scope

The criteria given below apply to the instrumentation and control installations executing instrumentation and control functions with safety significance on levels of defence 1 to 4.

The fulfilment of the criteria is realised by installations comprising hardware and software with I & C functions.

2 Categorisation

According to their safety significance, the instrumentation and control functions are classified into different categories to which graded criteria apply:

Category A
The instrumentation and control functions of Category A comprise all functions necessary to control events assigned to level of defence 3.

Category B
The instrumentation and control functions of Category B comprise all functions necessary to control events assigned to level of defence 2 and to prevent the occurrence of events assigned to level of defence 3.

Category C
The instrumentation and control functions of Category C comprise all other functions with safety-related significance.

Instrumentation and control functions possessing no immediate safety-related significance are not categorised.
N o t e: No criteria are specified in the following for instrumentation and control installations executing uncategorised instrumentation and control functions.

3 Design

3.1 Instrumentation and control installations for instrumentation and control functions of Categories A to C

3.1 (1) Instrumentation and control installations provided for the execution of instrumentation and control functions of different categories are planned and designed in accordance with the criteria of the category with the highest safety-related significance and are operated in accordance with the criteria of this category.

3.1 (2) Hardware has been reviewed for its suitability or has been proven by operating experience for operational mode and under the postulated ambient conditions, and is maintenance-free to the furthest possible extent.
Software is qualified for its suitability.

3.1 (3) Lines and cables including fibre-optic cables are arranged in separate redundancies and – wherever necessary – routed such that they are protected against internal and external impacts.

3.1 (4) The instrumentation and control installations are designed, assembled, shielded and protected such that any inadmissible influencing of the signals by internal as well as external interference sources is prevented.

3.1 (5) Measures and installations are provided making it possible to verify the operability of the instrumentation and control installations and their interaction with the active and passive components of the safety system and monitor the condition of these safety-related components.

3.1 (6) Signals from active components that have an effect on the operation of the instrumentation and control installations are preferably derived from the process variable or picked up directly from the drives, motors etc.

3.1 (7) Instrumentation and control installations executing instrumentation and control functions of Categories A and B are designed and operated such that their operability is ensured irrespective of the transient behaviour of the input signals.

The alarm systems are designed such that an overload of information is processed without any safety-relevant information being lost.

3.1 (8) Instrumentation and control installations are designed such that any necessary adaptations to regularly recurring conditions of normal operation of the plant (e.g. stretch-out operation) can be carried out easily and reliably.

3.1 (9) Instrumentation and control installations are designed such that they do not impair the independence and fault-tolerance of the corresponding active process systems.

3.1 (10) The accident-proof property of the instrumentation and control installations has been verified wherever necessary.

3.1 (11) The use of technical measures against operator failure is preferable to organisational measures.

3.1 (12) The instrumentation and control installations are designed such that manual overrides necessary for controlling events and for carrying out accident management measures are provided. These overrides are designed such that they will not impair the operability of the instrumentation and control installations for the control of events on level of defence 2 or 3 in an impermissible manner. Manual overrides are protected against operator errors.

3.2 Instrumentation and control installations for instrumentation and control functions of Category A

3.2 (1) The design of the instrumentation and control installations executing the instrumentation and control functions of Category A takes into account failure-initiating events within and outside the safety system.

3.2 (2) The stand-by positions of the equipment of the safety system can be changed only if corresponding release conditions are fulfilled and if these changes can be reversed again either automatically or by technical or organisational measures in case the release conditions are no longer fulfilled. Safeguards are provided against impermissible interventions when these systems are in stand-by position.

3.2 (3) If stand-by positions of actuators of the components of the safety system are specified for normal operation, consequently any departure from these stand-by positions is signalled.

3.2 (4) Instrumentation and control installations executing instrumentation and control functions of Category A are designed with sufficient reliability for ensuring their operability. Their design is conceived such that even in the case of maintenance of this equipment, the safety system will fulfil its function with sufficient reliability (see also "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components" (Module 10) Section 1.1).

a) The design of the instrumentation and control installations executing instrumentation and control functions of Category A is based on the principle of redundancy. They are physically separated or adequately protected and designed independently.
b) A failure in the instrumentation and control installations of the safety system can at the most have effects only on the function of the safety system redundancy affected.
c) The instrumentation and control installations necessary to ensure the operability of the safety system following the onset of events on level of defence 3 are designed in such a manner that they will withstand the respective most adverse ambient and accident conditions that may occur in the corresponding location.

3.2 (5) The instrumentation and control installations are designed that spurious actuation of the safety system is prevented under consideration of subsection 3.2 (11), if this may lead to beyond-design basis plant conditions.

3.2 (6) The instrumentation and control installations executing instrumentation and control functions of Category A are designed such that protective actions are on principle performed automatically.

Only if it is ensured that from the moment of recognition of an event on level of defence 3 up to the actuation of the necessary protective action there is sufficient time available for decision-making and for the performance of the protective action by the personnel are protective actions allowed to be actuated manually.

The design reference value for the time span within no manual actions are required is 30 minutes.

3.2 (7) The instrumentation and control installations executing instrumentation and control functions of Category A are on principle designed to be self-monitoring. The functions and properties not covered by the installations' self-monitoring are subjected to periodical and complete testing. The test cycles are defined on the basis of reliability analyses. These tests are to be easily carried out by means of in-built test aids at interfaces provided for it.

Test procedures and manual actions are designed such that necessary safety functions are neither prevented nor that the reliability of their actuation is significantly reduced.
N o t e : See also the criteria for ensuring the operability of safety-relevant installations according to the "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components" (Module 10) Section 1.4.

3.2 (8) Self-monitoring is designed in such a manner that it will not impair the function of the instrumentation and control installations executing the instrumentation and control functions of Category A. The regular tests according to subsection 3.2 (7) are planned and carried out in a way that no tests of redundant instrumentation and control installations will take place at the same time.

3.2 (9) The instrumentation and control installations executing instrumentation and control functions of Category A are on principle only used for tasks within the safety system. If installations executing instrumentation and control functions of Category A are also used for tasks on levels of defence 1 and 2, the associated instrumentation and control installations are designed in such a manner that the required reliability of the equipment executing instrumentation and control functions of Category A will not be impaired.

3.2 (10) Instrumentation and control installations executing instrumentation and control functions of Category A are designed such that the proof required for the qualification of the instrumentation and control installations of the safety system can reliably be furnished.

3.2 (11) The effects of systematic failures of instrumentation and control installations on event sequences on level of defence 3 are analysed taking into account the needs of the engineering systems.

The design of the instrumentation and control installations executing instrumentation and control functions of Category A provides measures against systematic failures of the hard-wired instrumentation and control installations for reducing the occurrence probability in such a way that they no longer have to be postulated.

The design of the instrumentation and control installations executing instrumentation and control functions of Category A provides measures against the systematic failures of the software-based instrumentation and control installations including systematic software failure in such a way that a systematic failure is controlled.

For software-based instrumentation and control, dissimilar instrumentation and control installations are used as a matter of principle. There are no requirements regarding the use of dissimilar installations if for the respective instrumentation and control function to be executed

– an active systematic failure is safety oriented, and
– if in case of a passive systematic failure the accident is controlled by other instrumentation and control functions of Category A executed by instrumentation and control installations being dissimilar to the installation failed.

For protective actions not being safety oriented for every plant condition, a 2-fold or 3-fold dissimilar design of the software-based instrumentation and control is used in dependence of the effects of passive or active systematic failures in the instrumentation and control installations executing instrumentation and control functions of Category A. A 2-fold dissimilar design is used
– if the accident is controlled with the still available safety installations under consideration of subsection 3.2 (6), or
– if each of the two dissimilar instrumentation and control installations triggers the required protective action on its own.

Should one of the two prerequisites mentioned for the use of a 2-fold dissimilar design not apply, a software-based instrumentation and control with 3-fold dissimilar design is used.

3.2 (12) The instrumentation and control installations executing instrumentation and control functions of Category A are principally designed in such a manner that they can fulfil their functions in case of demand under consideration of the following assumptions:
a) a random failure due to a single failure,
b) and a systematic failure (systematic failure of the hardware or systematic software failure), not applicable to hard-wired instrumentation and control if prerequisite of subsection 3.2 (11) is fulfilled,
c) and consequential failures
d) and in case of maintenance.

If demanded during maintenance, a systematic failure and a random failure are not postulated to occur simultaneously within a period of 100 h.

For software-based instrumentation and control installations with a sufficient degree of self-monitoring and maintenance times demonstrated to be less than 10 h, a random failure or the maintenance case is not postulated to occur simultaneously with systematic failure.

For failure due to single failure or unavailability due to maintenance, further criteria are specified in the "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, System and Components" (Module 10), Section 1.

3.2 (13) Protective installations for equipment and auxiliary equipment are designed in such a manner that in case of demand of the equipment by the instrumentation and control installations of the safety system, the protective installations will not become effective unless the possibly resulting consequential damages will put the plant's safety more at risk than the loss of this equipment.

The protective installations are principally designed in such a manner that priority of the instrumentation and control functions of Category A over the protective installations is ensured.

Wherever it is necessary that a protective installation has priority over instrumentation and control functions of Category A, the criteria of Category A apply to the protective installations.

The criteria of Category A for the protective installations do not apply if proof is furnished that failures of the protective installations are so unlikely that any resulting inadvertent actuations can be excluded.

3.2 (14) Instrumentation and control installations are designed in such a way that they will not have a determining effect on any safety system unavailability.

3.2 (15) Manual reactor scram is possible at any time during operating phases in which the availability of the reactor scram system is required, even in case of postulated systematic failure of software-based instrumentation and control including software failure (see subsection 3.2 (11).

3.2 (16) During operating phases in which part of the instrumentation and control functions of Category A are unavailable according to plan, reliable and effective accident control is ensured for the events postulated under these conditions during these operating phases.

3.2 (17) The instrumentation and control installations executing instrumentation and control functions of Category A are designed in such a way that even if the single failure to be postulated occurs in these installations, no actions will be triggered that could take the reactor to accident conditions.

3.2 (18) Actuation criteria for instrumentation and control functions of Category A and the protective actions and measures triggered by them are indicated clearly in the control room.

3.2 (19) The protective actions and measures triggered by the instrumentation and control functions of Category A together with their effects on the process are indicated in the control room and the emergency control room in a way that allows the operating personnel to check the condition of the plant reliably and in time.

3.3 Instrumentation and control installations for instrumentation and control functions of Category B

The instrumentation and control installations executing instrumentation and control functions of Category B are designed in such a manner that they can fulfil their functions even if upon demand an additional random failure occurs with resulting consequential failures.

An instrumentation and control installation which may initiate an accident by inadvertent excitation is superposed by an instrumentation and control installation being independent of the instrumentation and control installation assumed to have failed. The instrumentation and control function of this independent instrumentation and control installation is classified as Category B.

3.4 Instrumentation and control installations for instrumentation and control functions on level of defence 4

The instrumentation and control installations intended to execute the instrumentation and control functions for pre-planned measures on levels of defence 4a, 4b and 4c are designed in such a way that they will fulfil their function with a reliability sufficient for the respective level of defence under the ambient conditions postulated for the respective tasks. All instrumentation and control installation devices may be used for accident management measures if suitable.

4 Requirement specification for instrumentation and control installations used for instrumentation and control functions of Categories A to C

4 (1) All requirements for instrumentation and control functions of Categories A to C are documented and clearly presented in a requirement specification.

4 (2) The tasks of the instrumentation and control functions used on levels of defence 2, 3 and 4a are determined on the basis of an analysis of event sequences which comprises the events postulated on levels of defence 2, 3 and 4a.

For accident management measures, possible uses of the available instrumentation and control installations are considered.

4 (3) The requirement specification for the instrumentation and control functions of Categories A and B is structured such that the process engineering requirements are divided into clearly separated subtasks. These subtasks are represented by individual instrumentation and control functions.

The subtasks of the software-based instrumentation and control installations executing instrumentation and control functions of Category A are designed such that they have a small functional scope.

The entirety of all instrumentation and control functions is documented with a clear structure.

4 (4) For each instrumentation and control function, the tasks, allocation to Categories according to Chapter 2, actuation criteria, input signals, signal conditioning, control of actuators, alarms/indicators, data storage and interfaces to other instrumentation and control functions are indicated.

4 (5) It is shown that the instrumentation and control functions ensure compliance with the protection goals in all postulated events and event sequences in line with the requirement specification.

4 (6) The safety-relevant functions of the process control and information installations are defined in the requirement specification.

5 Monitoring of process variables

5 (1) Process variables necessary for the postulated events on levels of defence 2 to 4a as well as for the measures of plant-internal accident management (accident management measures) are monitored.

5 (2) For each event on level of defence 3 that is to be controlled by the instrumentation and control installations executing instrumentation and control functions of Category A, at least two different actuation criteria are used as a matter of principle which are based on physically different process variables. If not technically feasible, other measures and installations are provided to achieve a high degree of reliability.

6 Redundancy and independence

6 (1) Instrumentation and control installations are structured in such a way that the redundancy required for the active installations of the safety system remains ensured.

6 (2) Redundant instrumentation and control installations are designed to be independent of each other in a way that a plant-internal failure-initiating event will not lead to the failure of several redundancies. If individual redundancies of instrumentation and control installations executing instrumentation and control functions of Category A fail due to external impacts, the remaining redundancies will suffice to control this event.

6 (3) To prevent failure-initiating events affecting multiple redundancies within the instrumentation and control installations and within the plant, redundancies are on principle accommodated physically separated from each other.

6 (4) Connections of instrumentation and control installations executing instrumentation and control functions of Categories A and B with uncategorised equipment or with data processing or data transmission equipment of Category C are restricted to a minimum and demonstrated to be arranged to have no retroactive effects.

6 (5) The instrumentation and control installations executing instrumentation and control functions of Categories A to C are designed independent of each other to such a degree that if any failure-initiating events occur in installations of lower-ranking safety-related categories, the functions of the respective higher-ranking safety-related category remain ensured.

6 (6) The instrumentation and control installations executing instrumentation and control functions of Categories A to C are designed in such a manner that the output signals of installations of a higher-ranking safety-related category have priority over the output signals of installations of a lower-ranking safety-related category.

7 Qualification

7.1 Qualification of the hardware and the software of the instrumentation and control installations for I & C functions of Categories A to C

7.1 (1) In all phases of development, manufacturing, commissioning and operating of the instrumentation and control installations executing instrumentation and control functions of Categories A to C, administrative, design and analytical measures of quality assurance including testing are carried out and documented.

7.1 (2) The test of the instrumentation and control installations executing instrumentation and control functions of Categories A to C is performed during the manufacturing and assembly process with the integration of the system components. The individual system components are to be tested for system specification and implementation with regard to fulfilling the corresponding requirements for instrumentation and control functions placed on them.

7.1 (3) The instrumentation and control installations executing instrumentation and control functions of Categories A to C are comprehensively tested - under plant and operating conditions that are as realistic as possible - with respect to control all postulated event sequences.

7.1 (4) Following the installation in the plant or any modifications to the instrumentation and control installations executing instrumentation and control functions of Categories A to C, a commissioning test is carried out.

7.1 (5) The information systems are qualified according to their safety significance.

7.2 Qualification of the hardware

7.2 (1) For instrumentation and control installations executing instrumentation and control functions of Categories A und B, hardware is used that is reliable, type-tested or has been proven by operating experience under the postulated operating conditions and which is maintenance-free to the furthest possible extent.

7.2 (2) For instrumentation and control installations executing instrumentation and control functions of Category C, hardware is used that is reliable and qualified for the postulated operating conditions.

7.2 (3) The plant-specific qualification of the hardware is demonstrated by the comparison of its features with the criteria specified for its use in operation.

7.3 Qualification of the software

7.3.1 Software for instrumentation and control functions of Categories A to C

7.3.1 (1) The software is developed according to a phase model in individual verification steps.

7.3.1 (2) The software architecture is designed in such a way that the functions of the application software and the system software are realised in separate software modules and the application software is separate from the system software.

N o t e: The system software includes e.g. the operating system and – in the case of multiple-computer systems – the software for communication among the different computers.

7.3.1 (3) The software is designed such that there will be no inadmissible retroactive effects of the instrumentation and control installations of the lower-ranking safety-related category on the instrumentation and control installations of the higher-ranking safety-related category.

7.3.1 (4) The software is designed such that it is ensured that it will run in line with the requirements irrespective of the kind and scope of the time derivative of its input signals.

7.3.2 Software for instrumentation and control functions of Category A

7.3.2.1 Principles

7.3.2.1 (1) The development and qualification of the software for instrumentation and control functions of Category A are executed such that consistent safety demonstration of the correct operation of the software is ensured. The design and implementation are carried out by means of formalised and computerised design and test methods according to the state of the art in science and technology.

7.3.2.1 (2) The software for instrumentation and control functions of Category A is on principle simply structured.

7.3.2.1 (3) The functional range of the software for instrumentation and control functions of Category A is on principle limited to the degree necessary for the respective function.

7.3.2.1 (4) The software is designed to be robust and self-monitoring.

7.3.2.2 Quality assurance

7.3.2.2 (1) The software is developed consistently according to a phase model, using computerised tools.

7.3.2.2 (2) The software is built up from well-defined modules with limited functional range. These software modules are programmed as simply as possible, restricted to indispensable commands and interfaces, and are integrated in a clear program structure.

7.3.2.2 (3) The results of the individual software development phases are fully verified by application of formal analysis methods and additional tests whether these requirements are fulfilled. For this purpose, tests are carried out at defined milestones.

7.3.2.2 (4) Following the installation of the software on the computers, the required behaviour of the hardware and software systems is validated. If validation is performed in several steps, the individual validation steps are designed to be overlapping.

7.3.2.2 (5) The organisation and administration of the software development ensure that the software is developed and used according to complete development, testing, maintenance, and quality assurance plans. The independence of design and quality assurance is consistently maintained. Full documentation is available on development, quality assurance, and use.

7.3.2.2 (6) The methods and procedures applied ensure consistent software configuration (configuration management).

7.3.2.3 Use of pre-developed software

7.3.2.3 (1) The use of pre-developed software – unless designed according to the criteria in Section 7.3.2.1 and 7.3.2.2 - is restricted to necessary parts, with software modifications being avoided. These parts are subjected to tests equal to the proof furnished in Section 7.3.2.1 and 7.3.2.2 as regards scope and detail.

7.3.2.3 (2) To judge the above-mentioned equal quality, the following are consulted:
- the software developer's references,
- the development documentation, user documentation, and QA documentation of the software,
- the results of independent software assessments (certificates),
- software operating experience, with consideration of application profiles,
- additional software tests.

7.3.3 Software for instrumentation and control functions of Category B

7.3.3.1 Principles

7.3.3.1 (1) For the development and qualification of the software of the instrumentation and control functions of Category B, descriptions and computerised test methods are applied supporting the verification of correct operation of the software.

7.3.3.1 (2) The software is designed to be robust and self-monitoring.

7.3.3.2 Quality assurance

7.3.3.2 (1) The software is developed according to a methodically adapted phase model, largely using computerised tools.

7.3.3.2 (2) The software is built up from modules that are clearly delimited with regard to their functions. These software modules are restricted to indispensable commands and interfaces, and are integrated in a clear program structure.

7.3.3.2 (3) The results of the individual software development phases are subjected to testing with subsequent documentation. A combination of test methods is applied so that all safety-relevant program parts are fully covered by functional tests.

7.3.3.2 (4) The required behaviour of the hardware and software systems is validated.

7.3.3.2 (5) The organisation and administration of the software development is such that it is ensured that the software is developed and used according to complete development, testing, maintenance, and quality assurance plans. The independence of design and quality assurance is consistently maintained. Full documentation is available on development, quality assurance, and use.

7.3.3.2 (6) Consistent configuration of the programs is ensured.

7.3.3.3 Use of pre-developed software

7.3.3.3 (1) The use of pre-developed software is restricted to indispensable components, with software modifications being avoided. These components are subjected to tests equal to the proof furnished in Sections 7.3.2.1 and 7.3.2.2 as regards scope and detail.

7.3.3.3 (2) In order to judge the above-mentioned equal quality, the following are consulted:
- the software developer's references
- the development documentation, user documentation, and QA documentation of the software,
- the results of independent software assessment (certificates),
- software operating experience, with consideration of application profiles,
- additional software tests.

7.3.4 Software for instrumentation and control functions of Category C

7.3.4.1 Principle

The software for instrumentation and control functions of Category C is qualified according to recognised methods of software engineering.

7.3.4.2 Quality assurance

7.3.4.2 (1) The different steps of software development are disclosed individually.

If possible, software tools are used for essential development steps.

7.3.4.2 (2) It is demonstrated by tests that phase targets have been reached. The tests are documented correspondingly.

7.3.4.2 (3) The required behaviour of the hardware and software systems is validated for the safety-relevant functions.

7.3.4.2 (4) The software is developed according to a quality assurance plan in line with sound engineering practice. Full development, quality assurance and user documentation is available.

7.3.4.3 Use of pre-developed software

For pre-developed software used, operating experience is documented or the software is certified.

The features required for assessing the applicability are documented.

8 Robustness

8 (1) For instrumentation and control installations, the electrical, electromagnetic, thermal, mechanical and radiation- as well as humidity-induced impacts are specified such that the postulated operating and accident conditions are covered reliably.

8 (2) Handling and maintenance are designed such that the safe functioning of the instrumentation and control installations executing instrumentation and control functions of Categories A to C is not inadmissibly impaired.

8 (3) The instrumentation and control installations needed for the execution of measures within the framework of accident management are such that they will not lose their required operability as a result of the consequences of the event sequences or plant conditions considered.

8 (4) The instrumentation and control installations executing instrumentation and control functions of Categories A to C are designed such that sufficient reserves are existing to accommodate ageing effects.

8 (5) The permissible voltage range for the instrumentation and control installations executing instrumentation and control functions of Categories A to C is not sensitive to excesses at both ends of the specified voltage range of the power supply.

8 (6) Instrumentation and control installations executing instrumentation and control functions of Categories A and B are designed to be fault-tolerant. Instrumentation and control installations executing instrumentation and control functions of Categories A and B are designed such that the failure behaviour is defined on principle and is safety-oriented as far as possible.

8 (7) The instrumentation and control installations executing instrumentation and control functions of Categories A to C are on principle designed such that no maintenance is necessary during power operation.

9 Maintenance and modifications

9 (1) The operability of the instrumentation and control installations executing instrumentation and control functions of Categories A to C is demonstrated by tests during the entire operating period of the plant. These tests cover all installations with relevant functions.

9 (2) The kind and scope of the tests as well as the time intervals between the tests are specified. These specifications are reviewed at regular intervals i. a. on the basis of operating experience.

9 (3) The results of the tests are documented.

9 (4) The instrumentation and control installations are on principle designed such that any changes caused by tests are reversed after the tests. Tests are carried out automatically or manually. The tests are planned and carried out such that the criteria of the "Safety Criteria for

Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, System and Components" (Module 10) subsection 1 (2) are fulfilled.

9 (5) Tests on instrumentation and control installations shall be monitored from central locations by the operating personnel in charge.

9 (6) Maintenance work is devised such that it can be executed without any inadmissible impairment of the plant's safety and that the effects of any postulated human errors will remain restricted to one redundancy.

9 (7) In case of any modifications of the instrumentation and control installations executing instrumentation and control functions of Categories A to C, at least the same quality standards are applied as to the design and manufacture of the instrumentation and control installations.

9 (8) In case of any modifications of the instrumentation and control installations executing instrumentation and control functions of Categories A to C, it is ensured that the parts modified fulfil their function and interact as required with the unchanged parts.

9 (9) Any modifications of the software of the instrumentation and control installations executing instrumentation and control functions of Categories A to C are made under observance of the quality criteria according to Section 7.3. Software modifications and the associated necessary intervention in the instrumentation and control installations are carried out such that the criteria of the "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, System and Components" (Module 10) Section 1.2 are fulfilled. Any intervention into the software is documented.

9 (10) Modifications of parametrisation data and the software of the instrumentation and control equipment executing instrumentation and control functions of Categories A to C are treated in such a way that they can be reconstructed. For this purpose, back-up copies are made at regular intervals prior to all modifications. Software and parametrisation data files are archived.

10 Criteria for access control

10 (1) Any intervention into the instrumentation and control installations executing instrumentation and control functions of Categories A and B is signalled in the control room. In cases where this is not technically possible, the control room personnel is informed about the intervention prior to the planned interventions.

10 (2) Unauthorised intervention into the instrumentation and control installations including the software is made difficult or prevented to the furthest possible extent, preferably by technical measures. Safeguarding by way of organisational measures is restricted to such areas where technical measures for safeguard cannot be used appropriately
The effectiveness and reliability of the measures and technical measures provided corresponds to the safety-related significance of the instrumentation and control installations.

11 Documentation

11 (1) The plant-specific configuration of the hardware and the software of instrumentation and control installations executing instrumentation and control functions of Categories A to C is documented over their entire life-cycle with regard to their as-is condition and any modifications made.

11 (2) The maintenance processes and any intervention into the instrumentation and control installations executing instrumentation and control functions of Categories A to C are documented.

11 (3) Operating experience acquired from the maintenance of the instrumentation and control installations executing instrumentation and control functions of Categories A to C is recorded, documented and systematically evaluated.

12 Power supply of the instrumentation and control installations with I & C functions of Categories A to C

12 (1) The instrumentation and control installations executing instrumentation and control functions of Categories A to C are supplied from uninterrupted power supply systems with energy storages. The capacity of the energy storages is rated such that under the assumption that the demand of electricity of a redundancy is covered exclusively by the energy storages assigned to it, the supply is maintained for at least 2 hours without falling below the minimal voltage limit. Following a complete loss of power or a drop below the minimum voltage limit, the instrumentation and control installations and their power supply are designed such that the instrumentation and control installations will be operational after voltage recovery.
N o t e: See also "Safety Criteria for Nuclear Power Plants: Criteria for Electric Power Supply“ (Module 12).

12 (2) The design of the power supply of the instrumentation and control installations executing instrumentation and control functions of Categories A to C is based on the same failure combinations as the design of the instrumentation and control installations to be supplied (see for Category A: subsection 3.2 (12) and see for Category B: Section 3.3).

12 (3) The design of the power generation equipment, the distribution networks and the instrumentation and control installations is adjusted such that the loads assumed for the instrumentation and control installations and the static and dynamic limits of the admissible supply voltages specified for the instrumentation and control installations are not exceeded.

12 (4) Any failures of the power supply of the instrumentation and control installations executing instrumentation and control functions of Categories A to C are detected and indicated by monitoring systems.

13 Accident instrumentation

13.1 Scope of accident instrumentation

The function of the accident instrumentation before, during and after
- an accident or
- an event that may lead to an increased release of radioactive materials into the environment of the nuclear power plant

is to allow an overview of the plant state and to display and timely document all important data describing the plant condition as well as the most important weather data.

13.2 General criteria for accident instrumentation

13.2 (1) The accident instrumentation is divided into accident display equipment and accident recording equipment.

13.2 (2) The components of the accident instrumentation system are designed to be accident-proof where necessary.

13.2 (3) The accident instrumentation equipment is connected to an uninterrupted emergency power supply of the emergency power system. For accident instrumentation equipment for which short-term unavailability is permissible due to their tasks to be performed, there is no necessity of uninterrupted power supply.

13.2 (4) The design concept and the safety-relevant details of the accident instrumentation are documented such that they are verifiable.

13.2 (5) The accident overview and wide-range display system and its recordings are designed as independent systems.

13.3 Accident instrumentation design

13.3.1 Accident display equipment

13.3.1 (1) The accident display equipment is designed such that the necessary data arising before, during and after an event on level of defence 3 or 4a and needed for the assessment of plant safety, the effectiveness of the safety system and for decision-making on accident management measures are indicated reliably and with sufficient accuracy.

The design of the accident instrumentation system takes into account that the relevant data arising before, during and after the onset of an event sequence or a plant state that may lead to an increased release of radioactive materials into the environment of the nuclear power plant (levels of defence 4b or 4c) and needed for decision-making on accident management measures are indicated with sufficient accuracy under the postulated ambient conditions.

13.3.1 (2) The accident display system is further divided into an accident overview display system, a wide-range display system, and an accident detail display system.

13.3.1 (3) The accident overview display system is designed such that the relevant measured parameters before, during and after the onset of an event on level of defence 3 or 4a that are needed for an estimation of the plant state and the radiological consequences for the environment are recorded.

13.3.1 (4) A wide-range display system is provided for measured parameters which characterise the representative event sequences and plant states derived from them on level of defence 4b and 4c (see "Safety Criteria for Nuclear Power Plants: Criteria for Accident Management" [Module 7], in subsection 3.3 (2)).

13.3.1 (5) The accident detail display system is designed such that the function of the active safety installations and their equipment, including the auxiliary systems needed to fulfil their functions, are monitored. For this purpose, instrumentation and control installations of all categories may be used.

13.3.1 (6) The equipment is type-tested or qualified for the operational case and for postulated operating conditions. This equipment is maintenance-free to the furthest possible extent.

13.3.1 (7) The equipment for recording, processing and documenting the measured parameters is constructed as simple as possible.

13.3.1 (8) The measured parameters of the accident overview and wide-range display system are on principle displayed both in the control room of the nuclear power plant and in the emergency control room.

13.3.1 (9) The operability of the accident overview and wide-range display system is neither impaired by events on levels of defence 3 and 4a nor by their consequences.

13.3.1 (10) Redundant data acquisition and data processing of measured parameters of the accident overview and wide-range display systems is not necessary if

- the information content of the measured parameters can also be imparted by measured parameters of other measured parameters of the accident instrumentation or by measured variables of equivalent instrumentation,
- the loss of measured values of measured parameters can in case of need be accepted for a certain period of time and if within this period and under the then prevailing conditions this failure can be corrected or an alternative solution can be implemented.

13.3.1 (11) The part of the equipment of the accident display system accommodated in the area that is not protected against external impacts is decoupled from the equipment accommodated in the protected area.

13.3.1 (12) The equipment of the accident display system is designed according to ergonomic aspects in such a way that the conditions for optimal safety-related behaviour of the operating personnel are ensured.

13.3.1 (13) The accident display system is designed such that complete testing is possible and that the tests can be easily performed.

13.3.1 (14) The operability of the accident overview and wide-range display equipment is verified by tests over the duration of the plant's operating life. These tests cover all components with relevant function.

13.3.1 (15) The kind and scope of the tests and the time intervals between them are specified.

13.3.1 (16) The results of the tests are documented.

13.3.2 Accident recording system

13.3.2 (1) The accident recording system is designed such that the parameters measured before, during and after
- an event on level of defence 3 or 4a or
- an event that may lead to an increased release of radioactive materials into the environment of the nuclear power plant (level of defence 4b or 4c)

are documented in a clear manner and correct time order.

13.3.2 (2) The accident recording system is designed such that the time reference for each measured parameter covered by the accident instrumentation can be determined from the associated documentation with such accuracy that establishing the time relationship with data from other information sources is possible.

13.3.2 (3) The recording equipment is designed such that the time behaviour of the measured parameters is recorded with the necessary accuracy.

13.3.2 (4) The accident recording system is on principle in operation at any time. Restricted operability (e.g. for necessary repairs) is admissible if on demand the necessary information is ensured by the part of the accident instrumentation system that is in operational condition. The complete operability of the accident recording system is re-established as soon as possible.

13.3.2 (5) Specifications are laid down which equipment of the accident recording system is operational during operating phases B-F of the plant.

13.3.2 (6) To prevent a systematic failure, at least two data storages are used for recording and storage of the accident sequence data. Any failure of storage equipment will be displayed.

13.3.2 (7) The accident records are kept secure. It is ensured that these data are neither modified nor deleted.

13.3.2 (8) The ambient conditions following the onset of an event on level of defence 3 will not lead to circumstances under which the information needed for an assessment of the accident is unavailable.

13.3.2 (9) The data equipment is well arranged as well as clearly and unambiguously marked.

13.3.2 (10) The measured parameters of the accident overview and the wide-range display systems are on principle recorded in the control room of the nuclear

F

MODULE 6
"Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation"

Contents

1 Objective and scope

1 (1) This guidance text contains criteria for safety demonstration and documentation.

Suitable demonstration methods are applied to verify fulfilment of the criteria specified in the "Safety Criteria for Nuclear Power Plants".

N o t e: In the following, general criteria are formulated for safety demonstration and documentation. Detailed criteria for safety demonstration regarding loss-of-coolant accidents can be found in Annex 1. Detailed criteria for the determination of differential pressures within the containment can be found in Annex 2. Detailed criteria for the determination of jet and reaction forces in the case of leaks in pressurised systems within the containment can be found in Annex 3. Further technical criteria may be found in the dedicated technical guidance texts.

1 (2) For safety demonstration according to the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1, subsection 5 (7)), both deterministic and probabilistic methods are applied:

The deterministic methods comprise

- the analysis of events and conditions by calculations,
- the measurement and the experiment,
- the engineering assessment.

The deterministic methods form the basis for the performance of system assessments.

1 (3) The safety demonstrations are documented in the form of demonstration documents. These are complete and comprehensible as well as verifiable.

2 Fundamental criteria for system assessment

2 (1) A system assessment serves in particular for identifying whether the quality criteria specified in the "Safety Criteria for Nuclear Power Plants" for measures and installations are fulfilled. It takes into account the requirements for sufficient effectiveness of measures and installations that result from the analysis of certain events or conditions by calculations.

2 (2) The performance of a system assessment requires an up-to-date compilation of safety-relevant information on the prevailing requirements for sufficient effectiveness and the condition of the safety-related measures and installations concerned and, where applicable, taking into account planned modifications, including information about the functions to be executed on the respective levels of defence or the safety-related functions to be fulfilled as well as information about their structure, layout and design.

2 (3) Any deviations of the existing condition of the safety-relevant measures and installations from the condition described in the licensing documents are documented and assessed.

2 (4) If relevant to the circumstances to be analysed from a safety point of view, the results of the evaluation of operating experience are included in the system assessment.

2 (5) System assessments are performed with the involvement of qualified personnel of the licensee.

3 Fundamental criteria for the deterministic analysis of events and conditions

3 (1) The analysis of events and conditions establishes whether the quantitative criteria made in the "Safety Criteria for Nuclear Power Plants" (compliance with acceptance criteria) are fulfilled.

3 (2) If safety demonstration is done by analysing events and conditions,

a) up-to-date compilation of safety-relevant information on the prevailing condition of the safety-related measures and installations concerned and, where applicable, taking into account planned modifications
b) validated analysis methods according to the criteria in Section 3.1 are used for the respective areas of application;
c) the analyses regarding selected initial and boundary conditions are based on the requirements listed in Section 3.2;
d) the uncertainties in connection with levels of defence 1 – 3 that are associated with the respective analysis results for the corresponding acceptance criteria are quantified and taken into account in their entirety according to Section 3.3 or taken into account according to Section 3.4;
e) the uncertainties in connection with level of defence 4 analysis are assessed with regard to the acceptance target.

3 (3) If safety demonstration is done by analysing events and conditions, the following is documented in particular:
a) the results of the examination of the applicability of data used that is not plant-specific;
b) the justification of the choice of the underlying impacts, events, operating phases and operating conditions with regard to the fulfilment of the respective acceptance criterion;
c) in the case of statistical methods being used for determining the uncertainty of the analysis results: the distributions used in the analysis for the relevant input parameters, their derivation and, if relevant, their dependencies according to subsection 3.3 (1).

3.1 Validation of analysis methods

3.1.1 Objective

3.1.1 (1) Analysis methods that are used for safety demonstration of the fulfilment of the acceptance criteria of levels of defence 1 to 4b are validated for their respective scope of application.

3.1.1 (2) If calculation methods are used for analyses concerning the effectiveness of mitigative accident management measures (level of defence 4c) according to the "Safety Criteria for Nuclear Power Plants: Criteria for Accident Management" (Module 7), subsection 4.2 (1), these have been validated for the respective scope of application.
N o t e: See "Criteria for Nuclear Power Plants: Criteria for Accident Management" (Module 7), Section 4.

3.1.1 (3) The validation of an analysis method comprises the examination of the scope of application of the method and of the agreement of the results that can be obtained by application of this method with comparative values obtained from
- experiments, plant operation, plant transients or other events,
- exact analytical solutions, or
- other validated analysis methods.

3.1.1 (4) An analysis method may be considered validated if
a) the results obtained with the method lie within the bandwidths of experimentally obtained results (see subsection 3.1.2 (2), or
b) the results obtained with the method show a systematic deviation from the comparative values which can be explained by a known, technically or physically appropriate correction, or
c) the applicability and sufficient accuracy of the method applied has been demonstrated for the respective application within the framework of the validation scope performed and documented.

3.1.2 Performance

3.1.2 (1) Validation is based on a sufficient number of comparative values. The necessary scope as well as the required quality (see subsection 3.1.2 (2)) of the comparative values depend on the scope of application of the analysis method.

3.1.2 (2) Concerning the relevant parameters, the experiments used for validation cover on principle the range of conditions under which the analysis method is to be used. Otherwise, the applicability of the experimental results to the scope of application is justified.

3.1.3 Documentation

3.1.3 (1) The documentation regarding validation contains:
- data relating to the comparative values used (according to subsection 3.1.1 (3)), for experiments, plant transients or other events, including data on the accuracy of the comparative values referred to,
- data on the validated scope of application of the analysis method,
- descriptions of the calculation methods and models used as well as of the input data.

3.2 Specifications regarding initial and boundary conditions as well as the scope of safety demonstration

3.2.1 Criteria regarding the different levels of defence

3.2.1 (1) For the demonstration of the support stability of structural components, whose collapse could lead to safety-relevant impacts, the static and dynamic, mechanical, chemical and thermal impacts are considered.

a) The impacts that may result due to the defined conditions, events and operating states on levels of defence 1 to 3 are assumed or superposed such that all impacts are considered conservatively.
b) Concerning impacts resulting from events on level of defence 4a, the permissible loading of the structural components may in principle be higher than compared with level of defence 3, but it has to be ensured that all relevant impact and resistance values are realistically taken into account.
c) The impacts that may result for the components due to the event sequences and conditions postulated on levels of defence 4b and 4c are assumed realistically.

3.2.1 (2) For the demonstration of the integrity and support stability of components, static and dynamic, mechanical, chemical, thermal and radiation-induced impacts are considered. Dynamic impacts are considered by way of conservative boundary conditions or by consideration of the reaction of the respective components affected.

a) The impacts that may result due to the conditions, events and defined operating conditions on levels of defence 1 to 3 are postulated or assumed to occur simultaneously such that all effects on the load-carrying cross-sectional areas are considered conservatively with regard to the damage mechanism to be covered. If demonstration methods based on linear-elastic material behaviour are used, it is shown that regarding the damage mechanisms to be verified, the loads are assessed conservatively, taking the application limits of engineering methods into account.
b) Concerning impacts resulting from events on level of defence 4a, the permissible loading of the components may in principle be higher than compared with level of defence 3, taking into account all relevant impact and resistance values realistically. In the weakest locations, the integrity of the load-carrying cross-sectional areas will be maintained, retaining the basic geometry.
c) The impacts that may result for the components due to the event sequences and conditions postulated on levels of defence 4b and 4c are assumed realistically, and the effects on the condition of the components are analysed correspondingly.

3.2.1 (3) Safety demonstration on levels of defence 2 to 4a extends from the occurrence of an event to reaching a controlled plant condition.

The analyses relating to the effectiveness of the measures provided on levels of defence 4b and 4c are carried out up to the point where the state of the plant that is relevant for the analysis is reached.

N o t e: Detailed criteria for the calculation of the radiological effects to demonstrate the limitation of radiation exposure of the public on levels of defence 1 to 3 are compiled in "Safety Criteria for Nuclear Power Plants: Criteria for Radiation Protection“ (Module 9), Annex 1.

3.2.1 (4) For the quantification of the uncertainties of results according to Section 3.3, measuring and calibration errors may be considered statistically. If safety demonstration is done conservatively according to Section 3.4, the maximum measuring and calibration errors are assumed.

3.2.2 Level of defence 1 (normal operation)

3.2.2 (1) With regard to the respective design limits, the entire range of operating parameters coming into question over the period of operation or of the cycle is considered, taking into account the possible changes and oscillations during normal operation as well as measuring and calibration errors in the relevant safety-related parameters.

3.2.3 Level of defence 2 (abnormal operation)

3.2.3 (1) Adverse initial conditions lying within the range of realistic operating conditions are postulated for the different operating phases with regard to the respective acceptance criteria.

3.2.3 (2) All measures and installations allocated to level of defence 2 and demanded according to the specifications can be assumed as being available for safety demonstration unless they are to be assumed to have failed due to the postulated event.

3.2.3 (3) A simultaneous failure in addition to loss of off-site power that is independent of the event need not be assumed.

3.2.3 (4) The decay heat is calculated according to DIN 25463, for non-recycled nuclear fuels according to DIN 25463-1 and for recycled nuclear fuels according to DIN 25463-2.

Regarding the quantification of the uncertainties of results according to Section 3.3, the precise calculation method according to DIN 25463-1 can be applied to non-recycled nuclear fuels.

For a conservative safety demonstration according to Section 3.4, one standard deviation is added, applying the simplified equation according to Annex A of DIN 25463-1 for non-recycled nuclear fuels.

3.2.4 Level of defence 3 (accident)

3.2.4 (1) Worst-case initial plant operating conditions of normal operation are assumed for the different operating phases with regard to the respective acceptance criteria.
For values of safety variables not triggering instrumentation and control functions of Category A or B, the most unfavourable safety-relevant operating limits and conditions with regard to the acceptance target defined in the plant operating procedures are assumed for the safety demonstration.

3.2.4 (2) For demonstration of the effectiveness of measures and installations on level of defence 3, the single-failure concept according to the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1), subsections 3.1 (4) and "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components" (Module 10) is applied.

The postulated failures according to the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1), subsections 3.1 (7), 3.1 (8), 3.2 (6) and 3.2 (7) are taken into account.

3.2.4 (3) Loss of auxiliary power supply after turbine trip is postulated for all measures and installations necessary for accident control if this will have an adverse effect on the event sequence. Emergency power supply is considered in the analysis according to the switch-on programme of the equipment units supplied with emergency power.

3.2.4 (4) The decay heat is calculated according to DIN 25463, for non-recycled nuclear fuels according to DIN 25463-1 and for recycled nuclear fuels according to DIN 25463-2.

Regarding the quantification of the uncertainties of results according to Section 3.3, the precise calculation method according to DIN 25463-1 can be applied to non-recycled nuclear fuels.

For a conservative safety demonstration according to Section 3.4, a value of twice the standard deviation is added, applying the simplified equation according to Annex A of DIN 25463-1 for non-recycled nuclear fuels.

3.2.4 (5) Regarding loss-of-coolant accidents, the respective worst leak/break location is determined and postulated for the spectrum of the leak/break sizes to be considered for the respective individual safety demonstrations when determining the effects of

- the pressure and temperature build-up in the containment,
- the pressure differences in the containment,
- missiles, jet forces and reaction forces, and
- pressure blast waves within the reactor coolant pressure boundary.

as well as

- when demonstrating the effectiveness of the emergency cooling installations and the support stability of installations (especially large components) and rooms.

N o t e: On this issue, see also "Safety Criteria for Nuclear Power Plants: Events to be Considered in Pressurised and Boiling Water Reactors“ (Module 3) Annex 2 in addition to Annexes 2 and 3.

3.2.4 (6) In addition to the assumed failures of the single-failure concept, safety demonstration also takes into account accident-induced consequential failures of measures and installations with an adverse effect on the accident sequence as defined by the acceptance target.

In the event that this results in relevant adverse influences on the event sequence, it is postulated that the measures and installations on levels of defence 1 and 2 will become operative as specified.

3.2.4 (7) Combinations of several natural or other external impacts that are allocated to level of defence 3 or combinations of such impacts with plant-internal events are postulated in accordance with the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1), subsection 4.1 (5).

The accidental impacts and the impacts resulting from the accident consequences are combined with the "normal external operational loads" (incl. snow and wind loads) and the "forced reactions under normal operational loads". Consideration of the time-dependent progression of events is admissible for these combinations.

3.2.4 (8) As event-induced consequential events relating to external impacts, the possibilities for

a) impacts from burst pressure blast waves upon the failure of vessels with high energy content, unless the corresponding vessels are designed to withstand the impacts from the respective events;
b) consequential mechanical damage upon the failure of plant components;
c) flooding due to the failure of plant components and
d) fires

are considered, and

e) equipment malfunctions in plant areas that have not been correspondingly designed, with consideration of instrumentation and control installations and
f) loss of off-site power

postulated.

3.2.4 (9) The source term for radiological safety demonstrations on level of defence 3 is determined up until the end of the release. If necessary, suitable termination criteria are specified for defining the end of the release.

N o t e: Detailed criteria for safety demonstration in connection with loss-of-coolant accidents are compiled in Annex 1.

Detailed criteria for the calculation of the radiological accident consequences for safety demonstration of the limitation of radiation exposure of the population on levels of defence 1 to 3 are compiled in the "Safety Criteria For Nuclear Power Plants: Criteria for Radiation Protection “ (Module 9), Annex 1.

3.2.5 Level of defence 4a (anticipated transients without scram, man-made hazard conditions)

3.2.5 (1) When analysing anticipated transients without scram and man-made hazard conditions,

a) realistic initial and boundary conditions can be chosen;
b) all measures and installations that have not failed due to the postulated event can be assumed to be available;
c) the changes in operating parameters and conditions that are caused by instrumentation and control processes are taken into account;
d) an independent simultaneous failure in addition to loss of off-site power is only assumed for man-made hazard conditions.

3.2.5 (2) In supplement to subsection 3.2.5 (1), the following applies to the analysis of anticipated transients without scram:

a) The initial condition assumed is quasi-stationary power operation at the most unfavourable point in time of the cycle, corresponding to a xenon concentration prevailing when reaching the desired load condition as scheduled .
b) Regarding reactivity feedback effects, values are applied that cover existing uncertainties.
c) If within the short-term range (until maximum pressure is reached) credit is taken of the switch-off of the main coolant pumps (PWR), this is excited by instrumentation and control functions of Category A or B.

3.2.5 (3) The protection of building structures and components under man-made hazard conditions is verified on the basis of specified load assumptions. Here, induced structural and component vibrations are also considered.

3.2.5 (4) Combinations of several external impacts that are allocated to level of defence 4a or combinations of these impacts with internal events (e.g. pipe break, internal fires, smoke emission, loss of off-site power) are postulated if the events to be combined may show a causal relationship or if their simultaneous occurrence has to be postulated according to probability considerations (see also "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1), subsection 4.2 (3).

3.2.6 Level of defence 4b (events involving the multiple failure of safety installations) and level of defence 4c (accidents involving severe core damage)

3.2.6 (1) For the analysis of the effectiveness of preventive or mitigative accident management measures, realistic models and realistic initial and boundary conditions can be used for the event sequences on which they are based.

N o t e: Criteria for these levels of defence are compiled in "Safety Criteria for Nuclear Power Plants: Criteria for Accident Management“ (Module 7).

3.3 Quantification of the uncertainties of results

3.3 (1) The overall uncertainty of the respective analysis result is quantified according to subsections 3 (2) d). For this purpose,

a) the parameters (initial and boundary conditions as well as model parameters) and models that have a considerable influence on the uncertainties of the results are identified;
b) the ranges of uncertainty of the parameters identified that exist according to current knowledge are quantified, together with the parameter distributions if statistical methods are applied and,
c) where applicable, dependencies or interactions between individual input parameters are established and taken into account.

3.3 (2) Uncertainties of individual models not covered by a variation of parameters in the computer code, are covered by biases added to the result which are derived from the validation of the analysis method.

3.3 (3) If statistical methods are applied for the determination of the overall uncertainty, the unilateral tolerance limit in the direction of the acceptance criterion is determined, with a probability of at least 95% with a statistical confidence level of at least 95% shown for the fulfilment of the acceptance criterion.

3.3 (4) The compliance with statistical acceptance criteria is shown with a statistical confidence level of at least 95%.

3.4 Conservative safety demonstration

3.4 (1) The overall uncertainty according to Section 3.3 need not be determined

a) if methods or data that have been backed up by standardisation exist from which the uncertainty or a reliable margin to the design limit or the acceptance criterion can be derived, or
b) if the uncertainty can be considered by biases that have been derived from experiments or measurements and which are added to the analysis result, or
c) if the most unfavourable values of the uncertainty range of the individual parameters regarding the respective acceptance criterion are combined (taking model uncertainties into account); this method may only be applied if the result is a monotonously rising or falling function of the input parameters, or
d) if sufficiently conservatively chosen individual parameters are used for which it has been shown in a comparable case that the uncertainties quantified according to Section 3.3 are bounded for the respective acceptance criterion.

4 Fundamental criteria for safety demonstration by measurements

4 (1) Prior to the performance of measurements and experiments, the demonstration subject is specified and the measuring and experimental procedure planned in detail. If measurements or tests are to be performed within the nuclear power plant, the effects of the measurements or tests on the plant's safety are checked and set forth in writing. Safety-relevant adverse effects are prevented.

4 (2) If measurements or experiments are to be performed not within the plant or facility to be assessed but e.g. on component prototypes or test facilities, applicability to the components, systems or system functions to be assessed is justified. Any uncertainties in connection with the application of the results are identified.

4 (3) Safety demonstration by measurements and experiments takes measuring uncertainties into account. Deviations of the measurement or experiment from the process analysed in real operation are identified and considered in the safety demonstration.

4 (4) The demonstration subject, the measuring or experimental procedure and the results are documented in a comprehensible manner.

5 Fundamental criteria for engineering assessments

5 (1) Results from engineering assessments may be used for demonstration if:

a) a set of criteria exists for the safety demonstration subject and is used as a basis for the assessment; this set of criteria rests on technically and scientifically comprehensible fundamentals; for the determination of the set of criteria, applicable rules or standards, assessment results relating to the same or similar subjects, experiment results and empirical values may also be used, and
b) the set of criteria developed according to subsection 5 (1) a) is documented in a comprehensible manner.

5 (2) There are the following criteria for the performance of engineering assessments:

a) boundary conditions applied for the assessment, such as results and data from earlier calculations and tests, are justified and documented,
b) the results of the assessments are documented completely and in a comprehensible manner,

c) if applied to interdisciplinary and complex issues, the engineering assessment is performed by a team composed in an appropriate manner.

5 (3) For ergonomic analyses of personnel actions, the tasks assigned to the personnel are divided into subtasks within the framework of a task analysis such that an assessment can be performed regarding the required reliability of the personnel action and the safety-related criteria.

The task analysis considers the aspects:
- required and available information for the person acting,
- required processes of information processing,
- required decisions and individual actions,
- time-dependent and spatial boundary conditions of the tasks.

6 Fundamental criteria for probabilistic safety analyses

6 (1) The fundamental methods and boundary conditions for the preparation of probabilistic safety analyses (PSAs) and the requirements on documentation are described in the “Guide Probabilistic Safety Analysis”.

6 (2) Qualified personnel of the licensee is involved in the preparation of probabilistic safety analyses.

6 (3) The required scope and level of detail as well as the scope of documentation of the results of a PSA for the assessment of safety-relevant effects of plant modifications (to measures, installations or operating mode) is cause-related.

6 (4) Probabilistic safety analyses referred to for assessments according to the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1), subsections 5 (11a) and 5 (11b), use up-to-date methods, models and data. The up-to-dateness of the PSA considers in particular the following aspects:
- safety-relevant modifications to measures, installations or the operating mode performed in the plant,
- safety-relevant events or effects having become known, and
- the plant-specific evaluation of operating experience with regard to reliability parameters of components or occurrence frequencies of initiating events.

7 Fundamental criteria for documentation

7 (1) All documents used during the planning, construction and operation of the plant for the licensing and supervisory procedure (safety documentation) are documented in a systematic and comprehensible manner. The degree of detail of the documentation is adapted to the safety-related significance of the contents of the documents.

7 (2) The documentation fulfils the following criteria:
- application of a clearance/licensing procedure that is commensurate with the relevance of the respective document,
- clear identification of documents,
- timely updating of documents, in particular in case of plant modifications,
- identification of modifications and of the revision status of documents,
- assurance of the availability of applicable documents at the respective equipment locations,
- timely adaptation of documentation required for operation management to the current plant condition and keeping it available in the area of the control room,
- assurance of legibility and visual clarity,
- clear and unambiguous specification of safety-relevant operative instructions,
- identification and distribution of external documents to the respective equipment locations,
- prevention of the use of outdated documents or documents that are no longer applicable.

7 (3) As for the different kinds of documentation, a distinction is made between "safety documentation" and "other documentation". The safety documentation is maintained and

archived according to defined rules. Rules for the maintenance and archiving of the other documentation are established.

7 (4) Stipulations for the different kinds of document, documentation, document management, archiving, responsibilities and examination are specified in a documentation system.

Annex 1

Detailed criteria for safety demonstration regarding loss-of-coolant accidents

A1 (1) To show the effectiveness of the emergency core cooling installations, calculatory-analytical demonstrations that are backed up by experiments are provided. Either the uncertainties of the analysis results are quantified according to Section 3.3 or a conservative safety demonstration is done according to Section 3.4, with the following underlying assumptions.

1. For both methods, the worst combination of the following is postulated:
a) single failure,
b) unavailability due to maintenance,
c) loss of off-site power,
d) initial power in the core (upon the onset of the accident, the most unfavourable values are assumed that can occur during specified normal operation with consideration of the limiting process variables regarding integral power, rod power, and power density distribution),
e) point in time of the cycle,
f) break location, and
g) break size and break type.

N o t e: Postulated leak cross-sections and breaks as well as further criteria for the boundary conditions of safety demonstration are contained in "Safety Criteria for Nuclear Power Plants: Events to be Considered in Pressurised and Boiling Water Reactors“ (Module 3).

2. For the quantification of the uncertainties of results according to Section 3.3, measuring and calibration errors regarding initial core power can be considered statistically.
3. If safety demonstration is done conservatively according to Section 3.4, the maximum measuring and calibration error regarding initial core power is assumed additional to the requirements according to subsection A1 (1) 1.
4. In the analysis of pump behaviour during the depressurisation phase and the refill phase, possible blockings of free cross-sectional flow areas in the reactor coolant pressure boundary by damaged unit parts are considered.
5. The mass flow resulting from the one-dimensional depressurisation calculation is reduced by 20% for the hot rod temperature calculation, with consideration of thermal-hydraulically-induced flow distributions and possible cooling channel constriction, as long as no dynamic calculations of cladding ballooning are performed.
6. To determine the suction head of the residual-heat removal pumps, calculations are based on the assumption of atmospheric pressure prevailing in the containment following switch-over to sump operation.
7. On calculating the time-dependent water level in the reactor building sump, the following is considered in particular:
a) the changes in the primary coolant volume upon temperature changes;
b) the fill level of the reactor coolant system,
c) the steam content in the containment atmosphere,
d) the wetting of surfaces in the containment,
e) splash water and water accumulations that reach the reactor building sump only with a delay or not at all.
8. The following is taken into account in the demonstration that core cooling is ensured for both the short and the long term:
a) any released insulation and other materials that may influence the mechanical stability of the sump strainers installed in the building sump and the cavitation-free operation of the residual-heat removal pumps as well as the functions of further installations necessary for controlling events, and
b) the influence of released insulation and other materials that are carried into the core.
The demonstrations are based on thermal-hydraulic boundary conditions which cover the leak sizes including the double-ended rupture of the main coolant line.
9. For the determination of the sufficient achievement and long-term retention of subcriticality, it is postulated for the PWR that the secondary-side content of a steam generator is mixed with the primary coolant and the coolant injected by emergency cooling.

A1 (2) The following is considered in connection with the demonstration that the hydrogen concentration in the containment will at no time during operation nor following a loss-of-coolant accident exceed the ignition limit (4% of hydrogen in the air), neither locally nor integrally:

1. hydrogen sources:
- radiolysis in the core,

- radiolysis in the sump,
- radiolysis in the spent fuel pool,
- metal/water reaction in the core,
- other metal/water reactions.

2. Hydrogen formation is calculated for at least 100 days after the onset of the accident. The assumption here is that the hydrogen originating from metal/water reactions is immediately released and distributed approximately homogenously. As for the hydrogen forming in the long run through radiolysis, it is assumed that it will be released continuously, e.g. with or from the coolant. The location of release is considered in the calculation.
3. As a net formation rate for radiolysis in the reactor core and in the sump, a G(H2) value of 0.44 molecules/100 eV is assumed (this value represents the experimentally backed-up upper bound of the formation rate for the expected effective radiation).
4. Effective decay heat of the core

a) The source of the radiolytically acting radiation at least assumed is the equilibrium core at the end of the cycle that corresponds to the intended burn-up strategy, with consideration of the fission material and fission product composition of the fuel elements in the core and of the activation products. The time function of the γ decay output is calculated according to subsection 3.2.4 (4)).
b) The share of γ decay output absorbed in the coolant is determined as a function of time. If simplified assumptions are necessary for the calculation (e.g. division into energy groups, simplification of the reactor core geometry), then it is shown that these assumptions lead to conservative results. Otherwise a time constant of 10% is applied.
c) The absorption of β radiation in the coolant need not be considered owing to the self-shielding effect.

5. As regards the effective decay output in the sump, values are applied relating to the fission products released into the coolant that correspond to the maximum admissible scope of fuel rod damage, as far as no lower value is proved by a damage extent analysis .
   For the radiolysis calculation it is assumed, following the Radiological Accident Calculation Bases, that the following fractions of the fission products released (referred to the inventory of the defective fuel rods) are contained in the sump water:

- 6% of the halogens, alkali metals (90% spontaneous deposition in the sump of the 1% released halogens, alkali metals and 5% by leaching during sump operation),
- 0.5% of the spontaneous solids (99% deposition in the sump of the 0.01% other solids and 0.5% other solids by leaching).

  Their γ and β radiation energy is 100 % absorbed by the sump water

6. For the calculation of the amount of zirconium reacting in the reactor core, the time-dependent and spatial temperature distribution is taken from the results of the emergency core cooling calculations.
7. Other metal/water reactions are not considered if it can be shown that they release no important quantities of hydrogen.

Annex 2

Detailed criteria for the determination of differential pressures within the containment

A2 (1) The determination of the differential pressures within the containment is based on the following requirements (see "Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System" (Module 4), subsection 7.3.1 (3)):

1. The initial condition assumed is the operating condition at 100% of the specified power.
2. In accordance with "Safety Criteria for Nuclear Power Plants: Events to be Considered in Pressurised and Boiling Water Reactors“ (Module 3) Annex 2 "Postulated Leak Cross-Sections and Breaks in the Reactor Coolant Pressure Boundary or the Pressure Retaining Walls of the External Systems", subsections 2.1 (7) and 3 (9), leak cross sections up to 2A are postulated for the reactor coolant lines.
3. If lumped-parameter models are used, a sufficiently fine nodalisation is chosen (at least one zone for each room considered).
4. Regarding the release of the energy and mass contents defined according to the "Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System" (Module 4), subsections 7.3.3 (1), (2), and (3) the maximum possible release rates at the start of the outflow process are postulated.
5. For each room the least favourable break situation is considered.
6. Heat transfer to the structures is determined conservatively. If experimentally evidenced heat transfer relationships are applied, the lower values of the existing range of uncertainties are considered.
7. The flow resistances occurring during the course of the overflow processes between the different rooms are considered realistically but assumed conservatively for the room in which the break is located. The assumptions taken are evidenced by experiments.
8. If calculation models are used to determine water transport and moisture separation processes that consider these processes by empirical constants, then these constants are specified conservatively for the differential pressure behaviour.
9. Assumptions that are not evidenced by experiments are made conservatively.
10. The added safety margin of the thus calculated maximum occurring differential pressures is at least 15%. A value of at least 104 Pa is postulated for the differential pressure.

Annex 3

Detailed criteria for the determination of jet and reaction forces in the case of leaks in pressurised systems within the containment

A3 (1) The determination of effects caused by jet and reaction forces as well as by missiles on pressurised systems within the containment according to the "Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System" (Module 4), Sections 2 and 3, is based on the following requirements (see Module 4, subsection 7.3.1 (3)):

1. The initial condition assumed is the operating condition at 100% of the specified power.
2. For the selection and size of leaks, the assumptions according to the "Safety Criteria for Nuclear Power Plants: Events to be Considered in Pressurised and Boiling Water Reactors“ (Module 3) Annex 2 "Postulated Leak Cross-Sections and Breaks in the Reactor Coolant Pressure Boundary or the Pressure Retaining Walls of the External Systems" apply. For these leaks, a static outflow is assumed for various break locations.
3. Free jet propagation and repercussions on structures lying in its way are considered.
4. The respective worst break location is chosen.
5. To calculate the reaction forces of the pipes, corresponding calculation models or experimentally evidenced relations are applied.
6. An added safety margin of 15% is to be applied with regard to the loading of the relevant safety-related plant components by jet forces and by the structural parts accelerated by these jet forces.

G

MODULE 7
"Safety Criteria for Nuclear Power Plants: Criteria for Accident Management"

Contents

0 Objectives and scope

This guidance text contains the safety-related criteria for the planning, systems and provisions, safety demonstration and the personnel and organisational prerequisites of accident management.

1 General criteria for accident management

1 (1) The objective of the preventive measures of accident management is to reach long-term compliance with the protection goals in case of events with multiple failure of safety systems (see also “Criteria for Nuclear Power Plants: Fundamental Safety Criteria” [Module 1] in subsection 2.3 (3)).

The objective of the mitigative measures of accident management is to maintain the integrity of the containment for as long as possible, to retain the radioactive materials to the furthest possible extent and to reach a long-term controllable condition in case of accidents with severe core (see also “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ [Module 1] in subsection 2.3 (4)).

1 (2) The measures of accident management are oriented on the capabilities of the plant design (see also “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ [Module 1] in subsection 3.1(11)). The precautions are laid down plant-specifically.

Accident management is based on measures, installations specially provided for it, including not permanently installed (mobile) equipment and required interventions in instrumentation and control installations, as e.g. the reactor protection system, as well as on the flexible use of available safety and operating systems and the emergency systems provided for the control of specific very rare events.

When using accident management measures, these are given priority over competing actions of the reactor protection system, the component protection and the interlocking devices.

1 (3) The accident management measures to be applied in case of demand are selected in a symptom-based manner.

The objective of planning of accident management measures is to cover a broad spectrum of beyond-design basis event sequences, and phenomena in case of accidents with severe core damage with a limited number of measures.

Here, the event sequences and phenomena that, according to the results of the probabilistic safety analyses, make a dominant contribution to the core melt frequency and, in particular, those leading to the release of radioactive materials into the environment are taken into account.

1 (4) Accident management is based on accident management strategies and comprises accident management measures as well as accident management guidelines:
- Accident management strategies are written instructions for the use of preventive and mitigative accident management measures and accident management guidelines.
  The preventive accident management strategies describe the use of accident management measures and accident management guidelines to re-establish and to maintain the protection goals –reactivity control, fuel cooling, confinement of radioactive materials – in the long term.
- Preventive and mitigative accident management measures comprise special pre-planned plant-internal measures and / or installations.
- Accident management guidelines describe generic procedures that may be used if no accident management measures have been planned for event sequences and plant conditions or accident management measures are not effective as planned.

Possible positive and negative consequences of the performance of accident management guidelines are pointed out.

Note: For radiological criteria, see “Safety Criteria for Nuclear Power Plants: Criteria for Radiation Protection“ (Module 9).

2 Plant conditions, event sequences and phenomena considered in accident management planning

2 (1) Accident management measures are planned such that they are effective for a broad spectrum of beyond-design basis event sequences and phenomena in case of accidents with severe core damage.

2 (2) The planning of accident management measures is based on representative event sequences according to subsection 2 (4) and plant conditions derived from them..

For the determination of the representative event sequences, the results from the deterministic and probabilistic safety analysis operating experience as well as results of reactor safety research and international recommendations are referred to within the framework of an overall survey .

2 (3) For the derived plant conditions, criteria are defined for the selection, preparation, performance and control of the effectiveness of the appropriate accident management strategies.

2 (4) The representative event sequences on which the planning of preventive accident management measures is based comprise events in the following groups of events (see also "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1) subsection 4.3 (1)):

- transients,
- loss-of-coolant accidents inside the containment due to leaks in the reactor coolant system with a leak size ≤ 0.1 A (A: open cross-sectional area of the main coolant line),
- loss of coolant accidents with containment bypass,

1. in PWR plants due to an unisolable leak in pipes connected to the reactor coolant system,
2. in PWR plants due to steam generator tube failure with non-isolability towards the environment,
3. in BWR plants due to an unisolable leak in pipes connected to the reactor coolant system and due to unisolable leaks in the wetwell.

The effectiveness and feasibility of the preventive accident management measures is checked for the representative event sequences.

N o t e: For the planning of preventive accident management measures, the complete failure of one of the safety functions necessary to control the event on the one hand the failure of one of the necessary supply functions on the other hand are analysed separately. On this basis, the representative event sequences are determined which are taken as a basis for the planning of preventive accident management measures.

2 (5) For the planning of mitigative accident management measures, a spectrum of events is postulated that takes the relevant phenomena of accidents with severe core damage into account for the respective plant type. Here, accident sequences endangering the integrity of the reactor pressure vessel and accident sequences with containment bypass are considered.

2 (6) The planning of preventive and mitigative measures for the restoration and maintenance of fuel element cooling in the fuel pool is particularly based on event sequences with

- total loss of fuel pool cooling, and
- loss of coolant from the fuel pool with decrease of filling level below the minimum level required for cooling.

2 (7) For the planning of preventive and mitigative accident management measures, operating phases during low-power and shutdown operation are considered.

3 Criteria for accident management measures

3.1 Criteria for systems and provisions applied within the framework of accident management

3.1 (1) For the restoration or replacement of necessary safety functions, at least the following preventive accident management measures are implemented:

a) For PWR plants:
- steam generator feed after secondary-side bleed,
- reactor coolant system feed after primary-side bleed,
- reactor coolant system feed by high-pressure injection during sump operation;

b) for BWR plants:
- reactor coolant system feed with independent injection system,
- injection into the reactor pressure vessel by mobile devices,
- diversified pressure limitation of the reactor pressure vessel;

c) for PWR and BWR plants:
- assured containment isolation,
- provisions to ensure electrical energy supply.

3.1 (2) Objectives of mitigative accident management measures are at least:
- prevention of high-pressure failure of the reactor pressure vessel,
- prevention of overpressure failure of the containment due to continuous pressure increase and release limitation (filtered containment venting),
- prevention of combustion processes of gases (H2, CO) endangering the integrity of the containment),
- provisions to ensure electrical energy supply,
- sampling for diagnosis of the condition within the containment,
- assurance of working ability of the required personnel.

3.1 (3) The installations provided for accident management measures are designed such that the loads to be expected are transferred and the process engineering criteria are fulfilled.

3.1 (4) The installations taken into account within the framework of accident management guidelines may also be used beyond their design range if achievement of the objectives seems to be possible by doing so.

3.1 (5) The installations provided for accident management measures neither affect specified normal operation nor the deployment of safety installations in accordance with the design. Compatibility with the safety concept is ensured.

3.1 (6) For multi-unit plants, available means from other units may be used, provided that the safe operation of the other units is not compromised.

3.1 (7) For the installations provided for accident management measures there are no requirements for application of the principles of redundancy, diversity, segregation and physical separation (see “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" [Module 1] subsection 3.1 (3)).

Installations for depressurisation of the reactor coolant system are provided to perform accident management measures for depressurisation with a high degree of reliability (see “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" [Module 1] in subsection 3.4 (5)).

3.1 (8) The supply functions and handling equipment for the performance of accident management measures are available.

3.1 (9) The operability of the installations provided for accident management measures is ensured by maintenance and in-service inspections.

3.1 (10) The installations provided for accident management measures are designed such that they can be easily handled under the special conditions of the emergency situation.

3.1 (11) There is more time available for the preparation and performance of the planned accident management measures than required. The respective time available is determined such that the measure can be repeated if required. If the available times are too short, automations are made use of.

The necessary and available times are specified for the event sequences considered in the planning.

3.1 (12) For the planning of on-site manual actions, the environmental conditions to be expected when they are performed are taken into account.

3.1 (13) Measures for the repair of installations and for the restoration of lost safety functions may be considered in the planning of accident management measures.

3.2 Criteria for written instructions applied within the framework of accident management

3.2 (1) Accident management strategies, accident management measures, and accident management guidelines are specified in writing in the accident management manual (see “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" [Module 1] Section 5).

3.2 (2) The entry criteria for the accident management manual are defined.

Criteria are defined by which it can be determined whether the long-term fulfilment of the protection goals is ensured or a long-term controllable plant condition is reached.

3.2 (3) The accident management manual is developed according to ergonomic aspects with consideration of the special working conditions of the personnel during emergency situations.

3.2 (4) The accident management guidelines include criteria for the assessment of the plant condition that can be checked with the available instrumentation. If this should not be possible, the accident management guideline makes reference to other sources of information about the plant condition.

Positive and negative consequences of the measures to be considered are compared with regard to their effects. Here, long-term effects are also taken into account. For the successful implementation of prepared accident management guidelines, decision-making aids are developed, as far as necessary.

Decision-making aids are supporting documents that can be referred to for the application of the accident management guidelines.

3.3 Criteria for the provision of information, energy supply and communication

3.3 (1) Accident management measures are – as far as technically feasible – initiated and performed by the control room personnel.

3.3 (2) Information about the plant condition and the radiological situation at the plant as well as about the released amount and the environmental dispersion conditions are available in the control room and, as far as required, in the on-site emergency control centre.

The instrumentation allows the recognition of the plant conditions as well as the preparation, performance and control of the effectiveness of the accident management measures.

3.3 (3) The necessary precautions are taken to ensure the access and a long-term presence of the deployed personnel in case of an emergency at the locations provided for the preparation, performance and monitoring of the accident management measure.

3.3 (4) For ensuring effective work of the emergency response team, adequately equipped rooms supplied with energy are available at any time.

It is ensured that the rooms provided for the emergency response team are accessible under the conditions to be expected and that they are usable.

3.3 (5) In the event of a failure of the electrical power supply of the nuclear power plant including a failure of the emergency power generators (station blackout), the necessary power supply is available (see “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" [Module 1] Section 3.9).

For long-term back-up of energy supply, e.g. for charging of the batteries or supply of individual appliances, connection possibilities for external mobile devices are provided.

3.3 (6) The installations for sampling from the containment atmosphere and for coolant sampling provide information about the radioactive materials released into the containment and about the expected further development of the dispersion of radioactive materials.

This information is available to the emergency response team.

3.3 (7) Appropriate alarm systems and communication means are available by means of which instructions on how to behave can be given from at least one central point to the persons at the plant .

3.3 (8) Appropriate communication systems are provided for the performance of accident management measures as well as for communication.

For communication with external parties, e.g. authorities, technical advisors or aid organisations, communication systems are provided that are technically suitable and operable under the conditions to be expected.

4 Scope and criteria for safety demonstration

4 (1) The effectiveness of the preventive and mitigative accident management measures is demonstrated by appropriate methods for the representative event sequences considered.

4 (2) In case of any new findings and modifications of the plant or its operation, accident management measures are reviewed and, if required, updated or amended.

4 (3) The compatibility of the preventive and mitigative accident management measures with the implemented safety concept according to subsection 3.1 (5) is verified.

4 (4) The feasibility of the accident management measures is demonstrated and documented, e.g., by plant simulator exercises or emergency exercises.

4 (5) The general suitability and feasibility of accident management guidelines for achieving the protection goals is demonstrated.

4.1 Preventive accident management measures

4.1 (1) If deterministic analyses are applied for demonstration of the effectiveness of the preventive accident management measures, these may be performed with realistic models and realistic initial and boundary conditions for the representative event sequences considered.

Methods are used that are validated for the events and event sequences to be considered.

4.1 (2) For the demonstration of effectiveness, uncertainties of the analysis results are assessed with regard to the acceptance target (see also “Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation“ (Module 6), subsection 3 (2)e).

4.1 (3) The effectiveness of the preventive accident management measures is demonstrated for “transients” and in case of “loss-of-coolant accidents inside the containment due to leaks in the reactor coolant system“ 0.1 with a leak size ≤ 0.1 A (A: open cross-sectional area of the main coolant line) if it is demonstrated in the hot rod analyses that the following criteria are fulfilled in the long term:
- peak cladding temperature (PCT) < 1200 °C, and

– equivalent cladding reacted (ECR) (equivalent amount of the cladding consumed by oxidation) < 17%.

Regarding accident management measures for "loss-of-coolant accidents with containment bypass" according to subsection 2 (4), it is shown in analyses for the representative event sequences considered that during the event sequence no loads occur that lead to further event-based cladding damage.

4.1 (4) The effectiveness of the accident management measures for cooling of the fuel elements in the fuel pool is demonstrated for the representative event sequences considered if the fuel elements are covered with coolant.

4.1 (5) The effectiveness of the accident management measures for maintenance or restoration of the required subcriticality of the fuel elements in the reactor core and of the fuel elements in the fuel pool is demonstrated for the representative event sequences if long-term subcriticality of $k_{eff} < 0.999$ is maintained.

4.1 (6) For the representative event sequences considered, it is demonstrated that the loads occurring during the performance of the accident management measures do not endanger the integrity of the last barrier to be maintained or the effectiveness of the activity-retaining function.

4.2 Mitigative accident management measures

4.2 (1) If deterministic analyses are applied for the demonstration of the effectiveness of mitigative accident management measures, these may be performed with realistic models, realistic assumptions and boundary conditions for the representative event sequences considered (see also "Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation" [Module 6] in subsection 3.1.1 (2)).

4.2 (2) The effectiveness of the accident management measures for the prevention of high-pressure failure of the reactor pressure vessel by depressurisation of the reactor coolant system is verified if, for the representative event sequences considered, the pressure in the reactor pressure vessel is lowered such that endangerment of containment integrity is prevented in time by suitable measures.

4.2 (3) The effectiveness of the accident management measure of filtered containment venting is verified if it is shown for the representative event sequences and phenomena considered that the design pressure of the containment is not exceeded and effective depressurisation is possible. It is verified that no failure due to negative pressure occurs as a result of the filtered venting. It is shown that the release of radioactive materials into the environment is limited as far as possible by the use of appropriate filter systems.

It is shown that the conceptual design of the system and equipment provided is such that combustion processes of gases (H2, CO) within the system are prevented up to the stack outlet.

In BWR plants, the relief line is integrated in the gas space of the pressure suppression pool.

4.2 (4) The effectiveness of the accident management measures for prevention of combustion processes of gases (H_2, CO) endangering containment integrity is verified if for the representative event sequences and phenomena considered it is shown

– that combustion processes of gases (H2, CO) are generally prevented or that loads are prevented during possible combustion processes of gases (H2, CO) that lead to containment failure and
– that at the time of initiation of filtered containment venting in the area where the pressure relief line is connected with the containment, i.e. in the pressure relief line up to the first internal isolation valve, there are no explosive gas mixtures present.

5 Personnel and organisational criteria for accident management measures

5.1 Criteria for emergency organisation

5.1 (1) Personnel and organisational measures within and outside the plant supplement the technical measures for the prevention of severe core damage in case of events with multiple failure of safety systems and for mitigation of the consequences of accidents with severe core damage.

5.1 (2) Requirements on emergency organisation within the plant are stipulated in the form of written instructions. These cover, among other things, responsibilities, decision-making powers as well as criteria for measures within the plant, for convening of the on-site emergency response team and for alarming of the disaster control authorities.

Further, requirements are specified for measures of the personnel deployed by the licensee for the information and support of the authorities, in particular of the disaster control authorities.

5.1 (3) Plant-internal emergency organisation comprises the on-site emergency response team and the required shift personnel and deployed personnel of the licensee for performance of the measures as well as the persons for contact with external parties.

5.1 (4) The operational capability of the emergency response team and the personnel deployed of the licensee is ensured within a reasonable period of time after it has been convened so that the necessary measures can be prepared and performed. A period of one hour after alarming is applied as reference value.

5.1 (5) Preventive accident management measures are performed under responsibility of the shift supervisor until operational capability of the emergency response team is reached.

5.1 (6) In case that accident management guidelines or mitigative accident management measures become necessary under the responsibility of the shift supervisor before operational capability of the emergency response team has been reached, the respective proceeding is regulated.

5.2 Training and emergency exercises

5.2 (1) Qualification and targeted training and advanced training of the personnel oriented on coping with emergency situations is ensured for the respective tasks.

5.2 (2) The scope of training and the personnel to be involved in training and emergency exercises are specified.

5.2 (3) The programmes for training and advanced training of the personnel are systematically reviewed and updated with consideration of the actual plant condition as well as of the plant personnel's own experiences and experiences from other plants.

5.2 (4) For maintenance of the knowledge and skills of the personnel and for testing of the organisational processes, on-site accident management exercises are performed at least once a year.

In this respect, the procedure of convening the on-site emergency response team and the interaction of the deployed personnel required and the supporting organisations with the on-site emergency response team is checked.

5.2 (5) The authorities concerned in case of emergencies are involved in the emergency exercises to an appropriate extent.

5.2 (6) The emergency exercises are based on scenarios that adequately consider the plant's behaviour during event sequences up to and including accidents with severe core damage.

The scenarios and the course of the exercises are planned in detail.

The emergency exercises are close to reality. Here, simulators are also used as far as possible and appropriate.

The duration of the exercises is determined such that it is appropriate to the scenario selected.

5.2 (7) The emergency exercises performed are evaluated and included in a systematic experience feedback.

The course of the emergency exercises and the results of the evaluation are documented.

H

MODULE 8
"Safety Criteria for Nuclear Power Plants: Criteria for Safety Management"

Contents

1 Scope

The following criteria are applicable to the safety management of the licensee and the integrated management system serving its realisation.

The following safety-relevant criteria for the management system are applicable to the organisational units of the nuclear power plant and all other organisational units of the respective company that may have an influence on the safety of the nuclear power plant irrespective of the organisational structure of the company.

2 Objectives and fundamentals of the management of safety (safety management)

2.1 The prime responsibility for safety rests with the licensee. The licensee adheres to the safety criteria for nuclear power plants. He arranges for the development, introduction, implementation and review of a safety management. The licensee ensures that sufficient resources are available for it.

2.2 The safe operation of nuclear power plants requires a safety management that comprises the objectives and activities for a safety-oriented planning, organisation, management and control. The safety management ranges over the entirety of all activities and processes required for safe operation.

2.3 Safety management objectives are
- assurance and continuous improvement of safety, and
- strengthening safety culture

within a self-learning system.

The requirements for a nuclear power plant ensuing from acts, ordinances, rules and regulations, e.g. on safety, on environmental protection, on occupational health, on quality, on finances, are integrated into a management system.

All objectives and requirements ensuing from other objectives of the company (for example on quality, occupational safety, environment or economic efficiency) are in accord with the objectives and requirements of the safety management. All objectives and requirements are compared, weighted and clearly defined in a comprehensible and transparent manner under consideration that priority is given to safety.

N o t e: The international rules and regulations require the introduction of an integrated management system for ensuring safe operation of the plant. Only this way, the requirements made on the plant, as e.g. with regard to safety, environmental protection, occupational health and quality, can be considered systematically. Resulting conflicting objectives are then to be resolved at the process level. In the following sections, only those requirements for a management system are described that result from the aspect “assurance of safety. If conflicts of objectives are to be resolved, this is presented separately in the following.

2.4 The realisation of the safety management requires a management system that consistently describes and summarises, the specifications, regulations and means for planning, performance, review and continuous improvement of all activities and processes that may have an influence on the safety of the plant. An appropriate organisational structure, an appropriate procedural organisation and the resources necessary for safe operation are available.

3 Safety-relevant criteria for the management system

3.1 General safety-relevant criteria for the management system

3.1 (1) The management system promotes safety culture in particular by continuous learning and an open information exchange with regard to safety issues within the company across all levels of hierarchy. It contributes to a continuous improvement of safety and the safety awareness of the staff.

3.1 (2) The management system is adequate to give early indications of any potential impairments of safety.

3.1 (3) The management system is based on a process-oriented approach. In the management system, the closed management cycle is applied to all safety-relevant activities and processes. The closed management cycle comprises the phases of planning, performance, review and improvement (also referred to as PDCA cycle for “plan-do-check-act“).

3.1 (4) The development, implementation, review and improvement of the management system is an independent process which considers delimitations and interfaces, the coactions and potential interactions of the safety objectives and the safety-relevant requirements with those objectives and requirements on the management system resulting from other objectives of the licensee.

3.1 (5) Decisions that may have an influence on safety, are systematically developed, implemented, controlled and modified, if required. Potential impacts of decisions on safety are already taken into account during their development.

3.1 (6) The management system also considers external influences that may have an impact on plant safety (e.g. expectations of the public, competitive pressure).

3.1 (7) The management system includes the relationship with external organisations (e.g. manufacturers, suppliers, other contractors, supervisory and licensing authorities, experts, other nuclear power plants, operator organisations).

3.2 Safety policy and safety objectives

3.2 (1) The senior management defines the safety policy.
The safety policy is an integral part of the company’s overall policy and includes at least the following issues:

- Promotion of a highly-developed safety culture which permeates the entire company and whose continuous improvement is strived for.
- Priority of the safety objectives all other company’s objectives. In case of any unclear circumstances or assessment of the situation, decisions are taken in a safety-oriented manner.
- Operation of the plant in compliance with the legal requirements and those specified by the authorities, in particular those pursuant to the licence. The required demonstrations are provided.
- Provision of the resources required for the implementation of the safety policy during the entire operating life of the plant (see Section 3.7).
- Establishment, maintenance and further development of a transparent and adequate organisation for the promotion and realisation of the safe operation of the plant (see Sections 3.8 and 3.9).
- Systematic review and continuous improvement of safety.
- Information of the public.

3.2 (2) On the basis of the safety policy, unambiguous and measurable safety objectives that are neither in conflict with the safety policy nor with each other are derived for all processes of the company that may have an influence on safety so that the safety policy is implemented in the form of concrete specifications while first priority is given to the safety objectives.

A process is defined to incorporate changes of safety policy in the safety objectives.

3.2 (3) Regarding the implementation of safety policy and safety objectives, the senior management and the plant management level have a special responsibility. The senior management and the plant management level set an example of safety-oriented acting in order to strengthen and promote safety culture:

- They identify with and actively support the operating organisation's safety policy.
- They assume an exemplary and controlling function.
- They take the necessary measures that all staff comprehend contents and statements of the safety policy to a sufficient degree and that they are aware of their own function in ensuring safety.

3.2 (4) The senior management reviews the safety policy and the safety objectives at scheduled intervals and on occasions which put the safety policy and the safety objectives in question with regard to their effectiveness and completeness.

3.2 (5) On the basis of the results of the review, the senior management derives improvement measures for the safety policy and safety objectives.

3.3 Check of the effectiveness of safety management

3.3 (1) The senior management and the plant management level check the effectiveness of safety management by checking the effectiveness of all safety-relevant activities and processes as well as their coactions in the management system is checked.

3.3 (2) The scope of the effectiveness check is derived from the safety objectives and considers, in particular,
– all hierarchy levels of the company including the plant (senior management, plant management level, staff level),
– all internal interfaces between the different organisational units of the nuclear power plant and between organisational units of the nuclear power plant and other organisational units of the company,
– all external interfaces with authorities, expert organisations, contractors and other external organisations,
– the consistency of the results from the respective effectiveness check.

The measures of the effectiveness check are planned and performed independent of those involved in process execution.

The senior management and the plant manager evaluate the results of the effectiveness check in an appropriate manner and initiate improvement measures, if required.

3.3 (3) The effectiveness check concerns, in particular, the following aspects:
– completeness of the system with regard to the safety-relevant activities and processes,
– suitability of and compliance with the safety policy and the safety objectives,
– suitability of and compliance with the processes and their coactions,
– suitability for the identification of improvement potentials,
– comparison with the state of the art in science and technology.

For the effectiveness check, subsection 4.1 (3) is to be applied accordingly.

3.3 (4) The effectiveness is checked by
– independent internal or external reviews (such as management reviews and audits), and
– systematic comparisons with other plants and plant operators (as for example peer reviews).

3.3 (4) 1 At scheduled intervals, the senior management performs general reviews of the management system (management review) with appropriate methods. Here, the following aspects are particularly considered:
– the results of the review of safety-relevant activities and processes,
– the results of audits, reviews as well as systematic comparisons (benchmarking) and, where applicable, other internal or external reviews,
– the status of corrective and improvement measures,
– the status and the results of measures resulting from previous assessments,
– feedback from external organisations (authorities, experts, contractors, etc.),
– changes of internal specifications and external requirements.

3.3 (4) 2 The reviews required according to subsection 3.3 (1) are performed at adequate intervals and on special occasions.

3.3 (5) The senior management continuously improves the management system and its safety-relevant activities and processes, in particular, by

- implementation of the results from reviews according to subsection 3.3 (3) and 4.1 (3), and
- implementation of new findings resulting, in particular, from the evaluation of events and other experiences as well as from monitoring the state of the art and international safety standards.

3.4 Documentation of the management system

3.4 (1) The documentation of the management system comprises the following aspects:

- Scope of application of the management system,
- safety policy of the company and the plant,
- safety objectives of the company and the plant,
- derivation of process objectives and the safety-relevant processes,
- description of the safety-relevant processes and responsibilities for achievement of the safety objectives, including their justification ("know why"),
- processes for decision-making during comparison of safety objectives with other company's objectives,
- records for verification of conformity with the safety-relevant criteria of the safety management system,
- interactions of the safety-relevant processes and, where applicable, interfaces with and delimitations to other processes of the management system,
- indicators and measuring methods used for the effectiveness of safety management,
- results of the review of the safety management.

3.4 (2) Internal or external staff (contract personnel) concerned are informed about the available safety-relevant documents of safety management with respective explanations. This is done primarily after update or amendment of documents.

3.5 Responsibility of the senior management

3.5 (1) The senior management is responsible for

- the development and introduction of the management system that meets the requirements,
- the implementation of the management system under consideration of its influence on the safety and the safety culture in the company including the plant,
- the performance of regular reviews whether the specified requirements in the company including the plant are fulfilled,
- the resolution of conflicts of objectives between the different requirements for the company including the plant,
- the development of principles on the structural and procedural organisation,
- the provision of the necessary resources for the company including the plant.

Conflicting objectives between different requirements for the company as well as for the plant are resolved by the senior management in agreement with the plant manager.

The senior management sets an example of safety-oriented acting and actively supports it.

3.6 Responsibility of the plant manager

3.6 (1) The plant manager is responsible for

- the development and introduction of the management system at the plant,
- the implementation of the management system, including its influence on the safety and the safety culture at the plant,
- the resolution of conflicts of objectives between the different requirements for the plant,
- the development of the plant safety policy and objectives in compliance with the safety policy and the safety objectives of the company (Section 3.2),
- the establishment of the structural and procedural organisation (Section 3.8 and 3.9),
- the planning, performance, review and improvement of the management system, its documentation (Section 3.1, 3.3, 3.4 and 4.1) and related activities and processes, and
- the planning of resources (Section 3.7).

3.7 Provision of resources

3.7 (1) On the basis of a comprehensible procedure, the plant manager determines the resources required for the development, implementation, review and continuous improvement of plant safety with regard to the operating conditions and events to be considered on all levels of defence. The senior management ensures availability of the necessary resources. These comprise

- an adequate infrastructure,
- qualified and reliable personnel in sufficient numbers, including contract personnel (personnel resources),
- adequate working environment and working conditions,
- regulated co-operation with external organisations.

3.7 (2) The infrastructure needed for safe operation, implementation of the safety policy and achievement of the safety objectives is determined, specified, provided, maintained, controlled and improved, if required. Infrastructure includes the plant itself including its equipment (hard- and software), tools, auxiliary materials as well as supporting activities and processes (information, communication, transport).

The boundary conditions and the plant operating procedures for safe operation are specified.

The maintenance methods are specified to ensure the necessary effectiveness and reliability of safety-relevant measures and installations. The kind and frequency of maintenance and the verification of the operability of the infrastructure according to the requirements depend on its safety relevance.

3.7 (3) The number of staff and their competences required for the implementation of the safety policy, for achieving the safety objectives and for the performance of safety-relevant activities and processes are provided. Here, the number of staff and their competence resulting from the safety-related requirements for deputy and on-call regulations are also taken into consideration.

3.7 (3) 1 At the plant, there is always a sufficient number of qualified internal personnel in order

- to implement safety objectives and to specify safety-relevant activities and processes,
- to ensure specified normal operation (levels of defence 1 and 2),
- to ensure the control of design-basis accidents (level of defence 3) and to fulfil the safety-related objectives on level of defence 4
- to ensure understanding of the mode of operation of the plant for all plant conditions and to know and comply with the fundamentals of its licence
- to ensure experience feedback, knowledge management with knowledge preservation and transfer for all core competencies,
- to specify, manage and assess the work performed by external organisations.

3.7 (3) 2 For ensuring adequate competence of the personnel,

- a corresponding recruitment and selection procedure is applied by means of job specifications, defined prerequisites and appropriate pre-employment tests,
- the necessary social competencies (in particular, team behaviour, communicative competence, decision-making, leadership ability, attitude to work) of the personnel are also considered in addition to the technical qualification (education, practical experience and current technical knowledge),
- adequate processes for knowledge maintenance and transfer are established,
- all staff members are informed about legal and regulatory requirements, the plant's safety specifications, all rules governing the execution of safety-relevant activities, as well as about all new findings regarding safety. Here, the scope of the knowledge is oriented to the tasks of the respective staff member
- appropriate training is performed for all processes,

– training programmes are planned, performed, regularly reviewed for effectiveness by appropriate methods and continuously improved in a systematic and documented approach .

3.7 (3) 3 The plant manager is responsible for selection, employment and training of the plant personnel and thus for ensuring its necessary competencies in the long term.

3.7 (4) All measures, installations as well as auxiliary aids required for the performance of safety-relevant work are designed according to ergonomic principles of workplace design and the presentation of information.

The working environment and the working conditions are appropriate to ensure implementation of the safety policy and achievement of the safety objectives by the staff. In particular,
– they are adapted to the human abilities and the safety-related requirements,
– they are designed appropriate to the situation,
– they positively influence motivation, satisfaction and performance of the staff,
– they allow the work to be performed in a safe manner without any unreasonable physical and mental stress on the staff in all anticipated situations on levels of defence 1 to 4.

3.8 Organisational structure

3.8 (1) A an organisational structure is defined that complies with the safety policy and the safety objectives. Tasks, responsibilities and authorities (authority to make decisions and give instructions) are clearly allocated within the company, agreed with the executives of the different organisational units and communicated within the company. The responsibilities of the different organisational units are assigned without overlap and the interfaces defined, also involving the interfaces with external organisations.

The requirements ensuing from the procedural organisation are considered in the organisational structure.

Tasks are allocated such that there will be no conflicting interests for individuals. Delegation of responsibilities without gaps is ensured.

3.8 (2) The senior management delegates the task of managing the operation of the plant in a safe manner to the plant manager who is responsible for the safe operation of the plant. In the execution of his responsibility, the plant manger is assisted by the senior management. This also includes that planning and decisions of the company relevant to safe operation are made in agreement with the plant manager.

3.8 (3) “Officers” required by the authorities (e.g. radiation protection officers according to the Radiation Protection Ordinance (StrlSchV), nuclear safety officer according to the Nuclear Safety Officer and Reporting Ordinance (AtSMV)) are considered in the structural organisation according to their tasks and responsibilities.

3.8 (4) The organisational structure with the associated specifications is checked regularly with regard to the compliance with the safety policy and the safety objectives and improved, if necessary.

3.9 Procedural organisation

3.9 (1) The procedural organisation describes the safety-relevant activities and processes according to requirements of the management. For this purpose, all safety-relevant activities and processes are identified, their sequences, coactions and interactions defined.

The plant manager is responsible for all safety-relevant activities and processes in the plant as well as the required co-operation between all organisational units of the plant and with other organisational units of the company performing safety-relevant activities and processes.

3.10 Documentation of the resources and operation

N o t e: The general criteria for documentation are dealt with in "Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation" (Module 6), Section 7.

3.10 (1) The documentation of the resources is kept up to date. It includes

- the documentation of the safety-relevant infrastructure of the plant. This includes, in particular, a documentation of the respective actual plant condition including the documents for licensing of the plant with safety verifications, technical descriptions and documents on all modification measures performed,
- the
- regular documentation of the human resources available for all safety-relevant activities and processes,
- the safety-relevant specifications on the working environment and working conditions,
- the organisational structure of the company and the plant with organisation chart and descriptions for all organisational units that may have an influence on safety, and
- the safety-relevant regulations on the co-operation with external organisations.

3.10 (2) The main regulations on the organisational structure are included, for example, in the operating manual, accident management manual and testing manual. In addition to the technical processes, the regulations - in particular the procedural regulations – clearly define the respective competencies and responsibilities, review measures and quality requirements.

3.10 (3) The main regulations on the procedural organisation and on the operating modes are included, for example, in the operating manual, accident management manual and testing manual. The operational documentation comprises, in particular, the operating records, documents on regulatory procedures concerning licensing and supervision, analyses on own events and findings as well as from other plants, documents on maintenance experiences and results, the shift log, and information on amendments. The operational documentation is evaluated in a systematic and traceable manner. The results of the evaluation are considered in the planning and improvement of safe operation, including the management system.

4 Criteria for safety-relevant activities and processes

4.1 General criteria for safety-relevant activities and processes

4.1 (1) Planning of safety-relevant activities and processes

Safety policy and safety objectives are defined for the derivation of the objectives of activities and processes. The operative requirements on safety-relevant activities and processes are determined on the basis of the safety objectives under consideration of the following:

- The process objectives are defined.
- The safety-relevant requirements are assessed prior to their introduction and application in order to ensure that they are clearly defined and accomplishable.
- The requirements on activities and processes resulting from other objectives of the company are included. Competing requirements are regulated such that priority of safety-relevant requirements is clearly defined and comprehensible.
- The measures required to comply with legal and regulatory requirements as well as the plant's safety specifications during performance of activities are defined.
- Precautionary measures to avoid mistakes and to prevent the effects of any mistakes are defined.
- The required monitoring and review steps, with the associated criteria for the assessment of the safety-relevant process sequences and process results, are defined.
- The required resources for achieving the desired process results are defined.
- For all safety-relevant activities, the competent organisational unit is specified and, where applicable, reference is made to other activities or processes.
- For all activities and processes, the responsible personnel is defined.

4.1 (2) Performance of safety-relevant activities and processes

The performance of safety-relevant activities and processes comprises the following:
- Check whether the prerequisites for the performance of the activities and processes are fulfilled.
- Performance of the activities and processes according to the defined requirements and the regulations put in place.
- The flow of the activities is controlled and co-ordinated during performance, as far as required, the progress of the activities is documented and the traceability of the activities ensured.

Activities interrupted for safety reasons or other reasons are not resumed before the defined criteria are fulfilled under the given boundary conditions.

4.1 (3) Review of safety-relevant activities and processes

4.1 (3) 1 The performance and the results of all safety-relevant activities and processes is reviewed, taking into account that
- the activities and processes are performed according to the process specifications and the process objectives are achieved,
- the review of the respective safety-relevant activities and processes is performed on the basis of the documentation of the process and, where applicable, by other appropriate monitoring and measurement devices,
- the review is completed by the final determination of the process result.

Occasions, scope, frequency and methods of the reviews are defined.

The reviews are performed by the executing personnel and in dependence of the safety significance by the respective persons in charge.

4.1 (3) 2 Appropriate indicators and measuring methods for the review of safety.-relevant activities and processes are specified. The suitability of the methods is documented. The following is demonstrated:
- Stability, consistency and boundary conditions of data collection,
- suitability for trend tracking,
- the proper performance of data collection and data evaluation by qualified personnel.

4.1 (3) 3 Corrective measures to eliminate the causes of inadequate process results are taken so that recurrence is prevented. The development and the schedule for implementation of corrective measures are appropriate to the safety-relevant. The effectiveness of the corrective measures is checked.

4.1 (4) Improvement of safety-relevant activities and processes

A procedure for continuous improvement of the safety-relevant activities and processes is introduced. This procedure ensures that on the basis of the results of reviews, the assessment of operating experience and other findings according to Section 4.5 as well as other relevant information, the required measures are identified and implemented.

The senior management and the plant management level promote the commitment of the staff to actively participate in the development of improvement measures.

The improvement processes are co-ordinated to determine priority and resources. Priority improvement measures are determined on the basis of the safety significance.

4.2 Communication

4.2 (1) The senior management ensures that appropriate processes for communication within the company including the plant are available. The communication processes are maintained and their use promoted.

4.2 (2) Depending on the relevance of the information, communication may be formal or informal. For the communication from the managers as well as for the communication vice versa, there are systematised communication channels.

4.2 (3) The safety policy, safety objectives as well as the safety-relevant process objectives are communicated such that each staff member in the company can understand them to the required extent and is clearly aware of his/her role in ensuring safety.

4.2 (4) In all areas of the company including the plant, a trusting relationship with each other and open communication is cultivated and a culture is promoted that encourages and supports the exchange of safety-relevant information. The personnel is encouraged to give feedback on safety concerns.

4.2 (5) The company maintains communication relationships with external organisations (e.g. suppliers, regulatory authorities, expert organisations, other nuclear power plants, operator organisations, external contractors, such as suppliers, other companies) via well-defined and effective communication channels.

4.3 Safety-relevant modifications

4.3 (1) For each safety-relevant modification to the plant or its operation (e.g. installations, operating modes, structural and procedural organisation, instructions, review methods)
- an adequate assessment, verification and validation is ensured for each development phase,
- the responsible organisational units, their tasks and powers for planning, development and performance of modifications are specified. The interfaces between the organisational units involved are defined and described.

4.3 (2) It is ensured that by modification measures
- no impairment of safety is caused,
- the effectiveness of the management system is maintained and thus the safety-relevant objectives can be reached.

4.3 (3) For planning, implementation, review and improvement of short- and long-term modifications, a process is established that ensures the following under consideration of their safety relevance:
- feasibility considerations,
- substantiation and justification of the modification,
- design boundary conditions,
- safety considerations,
- update of documentation and training courses.

4.4 Co-operation with external organisations

4.4 (1) For the co-operation with licensing and supervisory authorities and expert organisations as well as the safety-relevant co-operation with external contractors and other external organisations, as e.g. other nuclear power plants and operator organisations, the necessary resources are provided and the processes are defined in an appropriate manner.

The delimitation and the interfaces as well as the coactions and the interaction with external organisations are defined under consideration of the safety relevance. .

4.4 (2) For the co-operation with the licensing and supervisory authorities and the expert organisations consulted by them, processes are established such to promote mutual understanding and to ensure the compliance with requirements specified by the authorities.

4.4 (3) The tasks of external contractors (e.g. manufacturers, suppliers and other companies) are defined and the requirements fulfilled by them specified under consideration of the coactions and interactions of the tasks.

4.4 (4) External contractors are assessed and selected according to specified criteria. The criteria regarding the competence of the personnel and the quality management of the external companies are defined. The assessment of the external companies is documented.

4.4 (5) The company continuously evaluates the experiences with external organisations with regard to the compliance with the safety and quality requirements. The senior management and the plant management level satisfy themselves that external contractors are able to fulfil the requirements to be applied to the resources to be procured (services, auxiliary materials, hard- and software).

4.4 (6) External contractors are included in the management system. The corresponding interfaces are defined in the management system. It is to be ensured that the contractor

- is sufficiently informed, and
- is trained and instructed.

The company reviews the required certificates of competence of the external contractor. The competencies are continuously assessed and monitored.

4.4 (7) The activities of personnel from other companies (contract personnel) are controlled and monitored by plant staff in order to ensure that the specified criteria are fulfilled.

4.4 (8) The contract personnel has the necessary competence and technical qualification for the tasks assigned to it.

4.4 (9) The company makes appropriate provisions to maintain the competent engineering and technical support provided by external contractors in all safety-relevant areas for the entire life of the plant.

4.5 Experience feedback

4.5.1 Processes and responsibilities

4.5.1 (1) The licensee ensures that reportable eventsin terms of the Nuclear Safety Officer and Reporting Ordinance (AtSMV), anomalies, operating experience, findings on safety-relevant aspects of the design of his own and other plants, changes in the state of the art and the international safety standards, including the information given on it as required by the authorities are registered, checked, evaluated and documented in a systematic manner in a process of the management system.

4.5.1 (2) The operating experience is evaluated in order to identify safety-relevant events so far unknown, precursor events and tendencies to the change in safety or of safety margins, as for example deficiencies with regard to infrastructure, operating mode and organisation.

4.5.1 (3) The senior management provides adequately qualified personnel for the performance of these processes and – as far as appropriate – for the recommendation of corrective measures. Relevant findings (indications, hints, results and trend) are reported to the plant manager.

4.5.1 (4) The personnel responsible for the task according to subsection 4.5 (1) 1 receive initial and advanced training, adequate technical and financial resources and support from the senior management.

4.5.1 (5) The plant manager ensures that results are achieved, conclusions are drawn and corrective measures are taken in a timely and appropriate manner to prevent any recurrence of events and to maintain or improve plant safety.

4.5.1 (6) The plant manager ensures that the competent supervisory authorities are informed about the relevant results and measures derived.

4.5.2 Reporting and dissemination of safety-relevant information

N o t e: Requirements for the reporting of events are regulated in the Nuclear Safety Officer and Reporting Ordinance (AtSMV).

4.5.2 (1) The plant manager requires all the personnel to report all safety-relevant events, anomalies and near-misses to the competent persons in the plant.

4.5.2 (2) The plant manager ensures that all reportable events are classified according to the International Nuclear Event Scale (INES).

4.5.2 (3) Safety-relevant operating experience and findings are exchanged between the competent personnel within the plant, communicated to the supervisory authorities and their authorised experts in an adequate manner and exchanged with other operators, operator organisations and international committees in an appropriate manner.

The senior management supports the supervisory authorities in the international exchange of operating experience.

4.5.2 (4) The plant manager ensures that the knowledge obtained from events, operating experience as well as changes in the state of the art are considered in the training programmes in an appropriate manner.

4.5.3 Evaluation of reportable events and other operating experience

4.5.3 (1) Safety-relevant events are evaluated without delay so that urgent measures that might be required can be taken immediately.

4.5.3 (2) The plant manager ensures that appropriate methods for the evaluation of reportable events and other operating experience are applied both to technical and human/organisational aspects.

4.5.3 (3) The evaluation of reportable events and other operating experience is performed according to their safety significance. The evaluation
- shows the entire course of the event,
- determines the deviation from the specified condition,
- identifies and analyses faults, causes and contributing factors,
- determines the safety significance including the potential effects,
- comprises the applicability to other systems and procedures under consideration of other boundary conditions,
- includes necessary corrective measures.

4.5.3 (4) The company maintains appropriate relations with the organisations that were and / or are dealing with the design and construction of the plant or technical installations to ensure experience feedback and to consult these organisations, if required.

4.5.3 (5) As a result of the evaluation of operating experience, the corrective measures are taken in a timely manner that are required to restore or to improve safety, to prevent any recurrence of events and to support safety-targeted trends.

Corrective measures are planned, performed, reviewed and documented according to the criteria of the management system.

4.5.4 Review and continuous improvement of the processes for the evaluation of reportable events and other operating experience

According to the criteria of the management system (see, in particular, Section 3.3 and subsection 4.1 (3) 2), the processes for the evaluation of operating experience and other knowledge obtained are regularly checked for their effectiveness. This may also be done by suitable external personnel. The results of the review are documented.

4.5.5 Documentation and archiving of operating experience

The plant manager ensures that the operating experience and other safety-relevant information are documented and archived such that it can be easily found and systematically searched, screened and assessed.

I

MODULE 9
"Safety Criteria for Nuclear Power Plants: Criteria for Radiation Protection"

Contents

0 Objective and scope, notes on placement and application

This guidance text contains criteria for occupational radiological protection and for the measures and installations in the area of radiation protection. Providing concrete specifications, they tie in on the one hand with the Atomic Energy Act and the Radiation Protection Ordinance as binding legal foundations and on the other hand touch the subjects of relevant guidelines, recommendations and technical rules which on their part have a higher degree of detail.

Since the guidance contained in the "Safety Criteria for Nuclear Power Plants: Criteria for Radiation Protection" (Module 9) ties in with the requirements anchored in the legal foundations, the present rules contain in part overlaps as regards content with the provisions of the Radiation Protection Ordinance wherever this is appropriate for an unambiguous and comprehensible phrasing of the guidance text. Passages of text containing overlaps as regards content with the Radiation Protection Ordinance are not to be understood as requirements in the sense of a double regulation but serve for the clarification of the reference made to the corresponding provisions of the Radiation Protection Ordinance.

Ordinances, general administrative provisions and guidelines will continue to be the standard for devising licences, requirements and regulatory measures. This also applies to federal supervision in the context of federal executive administration. The regulation contents of the guidance text therefore form a working basis for the regional radiation protection authorities of the *Länder* who adopt the criteria formulated in the guidance text for the area of nuclear engineering in additional requirements or in official orders and thereby accommodate the Radiation Protection Ordinance and the associated guidelines.

1 Limitation of radiation exposure

1 (1) In line with the provisions of the Radiation Protection Ordinance, the measures and installations for radiation protection are aimed at avoiding any unnecessary radiation exposure of the personnel, the population and the environment and at keeping any radiation exposure of the personnel, the population and the environment as low as achievable, taking into account all circumstances of individual cases. This objective is implemented in the design and in the operation of the plant on the basis of the requirements of the Radiation Protection Ordinance by

- the quality, layout and shielding of unit parts that contain or may contain radioactive materials,
- measures and installations by which the frequency and duration of tasks carried out by the personnel in radiation fields and the possibilities of personal contamination and incorporation are kept as low as achievable, taking into account all circumstances of individual cases,
- measures and installations for the safe handling of radioactive materials and for the treatment of radioactive waste and radioactive materials to be utilised without detrimental effects for storage within or dispatch from the plant,
- measures and installations by which the amount and concentration of radioactive waste as well as radioactive materials to be utilised without detrimental effects arising in the plant are kept as low as achievable, taking into account all circumstances of individual cases,
- measures and installations to prevent, limit or reduce the dispersion of radioactive materials through the plant or their release into the environment,
- measures and installations to prevent, limit or reduce the release of radioactive materials in the case of any safety-relevant events
- monitoring radiologically relevant parameters within the plant and in its vicinity.

1.1 Limitation of radiation exposure within the plant

1.1 (1) For the protection of plant personnel and contract personnel carrying out work within the plant on levels of defence 1 and 2,

- the number of persons tasked with the work,
- their individual dose, even below the limits stipulated in the Radiation Protection Ordinance, and
- the collective dose

are kept as low as achievable, taking into account all circumstances of individual cases, and any unnecessary radiation exposure or contamination is avoided.

1.1 (2) On level of defence 3, the plant personnel and the contract personnel is protected against event-induced radiological consequences by measures and installations in line with the relevant criteria of subsection 2.4 (1) of the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1).

For the planning of activities to control events on level of defence 3, to mitigate their effects or to eliminate the consequences of such events, the relevant criteria according to subsection 2.4 (1) of the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1) are applied as a basis regarding the radiation exposure of the personnel.

1.1 (3) According to the relevant criteria of subsection 2.4 (1) of the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1), measures and installations are provided to protect plant personnel and contract personnel

- against expected radiological consequences of events on level of defence 4a,
- within the framework of accident management, against expected radiological consequences of event sequences and plant conditions on levels of defence 4b and c.

For the planning of activities to control event sequences and plant conditions on level of defence 4, to mitigate their effects or to eliminate the consequences of such event sequences and plant conditions, the relevant criteria according to subsection 2.4 (1) of the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1) are applied as a basis regarding the expected radiation exposure of the personnel.

1.2 Limitation of radiation exposure in the environment

1.2 (1) On levels of defence 1 and 2, the radiation exposure of the population living in the vicinity of the site due to direct radiation and the release of radioactive materials from the plant is kept as low as achievable even below the admissible limits stipulated by the Radiation Protection Ordinance, taking into account all circumstances of individual cases. Releases due to events on level of defence 2 are counted among operational releases. The limits of the Radiation Protection Ordinance for the population are kept, taking into account the initial exposure due to the licensed release of radioactive materials from other nuclear facilities, due to the licensed handling of radioactive materials, and from earlier activities covered by the scope of the Radiation Protection Ordinance and as a result of activities in connection with the check-out of iodine therapy patients.

1.2 (2) By appropriate design, the radiological consequences of events on level of defence 3 are kept as low as achievable, taking into account all circumstances of individual cases.

The design for the protection of the population from release-induced radiation exposure is based on the maximum limits of the accident planning levels stipulated in the Radiation Protection Ordinance.

1.2 (3) For the events on level of defence 4a listed in the "Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors" (Module 3) as well as for the plant conditions, event sequences and phenomena to be considered for the planning of accident management measures (levels of defence 4b and 4c) according to Section 2 of the "Safety Criteria for Nuclear Power Plants: Criteria for Accident Management" (Module 7), measures are included in the planning to reduce the expected radiological effects to a level that is as low as achievable, taking into account all circumstances of individual cases, if a release into the environment cannot be excluded.

2 Organisational and personal radiation protection

2.1 Fundamental criteria

2.1 (1) For the implementation of the criteria according to subsection 1.1 (1), all persons with tasks to fulfil in the radiation protection areas behave according to the requirements of radiation protection. For this purpose,

- rules of conduct relevant to radiation protection are established in line with the radiation protection procedures required by the Radiation Protection Ordinance,

– the persons working in the controlled area are instructed on how to behave correctly,
– the aids needed for the planning and implementation of radiation protection measures are available,
– correct behaviour is promoted and checked.

2.1 (2) All-embracing organisational measures for the radiation protection of the personnel are laid down as part of the plant operating procedures (in particular, in the radiation protection regime). The radiation protection regime fulfils the requirements for radiation protection procedures according to the provisions of the Radiation Protection Ordinance.

2.1 (3) Experience with the operation of the plant is regularly evaluated with regard to the possible ways of further reducing the radiation exposure of the personnel, the population and the environment. Apart from the operating experience with the operator's own plant, experience available from comparable domestic and foreign plants is also considered.

2.1 (4) Possible ways of keeping radiation exposure as low as achievable, taking into account all circumstances of individual cases, are implemented by using existing measures and installations or, if necessary, by measures and installations to be newly devised. Apart from appropriate working methods, permanent installations for the retention of radioactive materials as well as for the limitation and reduction of direct radiation, contamination and airborne activity are primarily provided for this purpose. If necessary, mobile installations such as mobile shields, suction devices or decontamination facilities are also used. Personal protective equipment (e.g. respirators, protective clothing) is used if considering all circumstances of each individual case the requisite protective effect cannot be achieved by the above-mentioned structural and technical means.

2.1 (5) Successful implementation of the criteria according to Section 1.1 presupposes the active co-operation of all persons working in the controlled area to constantly improve radiation protection, which goes beyond the mere following of instructions. For this purpose, the continuous development of radiation protection is promoted as a part of safety culture, making use of the experiences and contributions of all those involved. In particular, the responsibility of each individual working in a plant to act and behave in a manner that is in line with the objectives of radiation protection is promoted and indeed demanded.

2.1 (6) Personnel tasked with work in controlled areas is informed about the radiological conditions and instructed with regard to correct behaviour. The necessary knowledge about suitable behaviour and protective measures is reliably imparted and practised as the need arises. The knowledge level of the personnel thus employed is updated by regular instruction at legally specified intervals.

2.2 Organisation of the radiation protection personnel

2.2 (1) The organisation of the radiation protection personnel is specified and documented in line with the provisions of the Radiation Protection Ordinance. These stipulations consider the radiation protection supervisor and the appointed radiation protection officers, the tasks, cognizances and duties they have been entrusted with as well as their in-plant authority.

N o t e: In practice, the following alternatives exist, depending on the organisational structure of the respective plants:

– a radiation protection officer, appointed by the radiation protection supervisor, with a number of deputies whose in-plant authority is clearly defined,
– several radiation protection officers, appointed by the radiation protection supervisor, each with his own defined in-plant authority and his own deputy.

In the further text of Section 2, the term "radiation protection officer" is used in the singular in the sense that the radiation protection officer in charge of the respective in-plant authority is referred to.

2.2 (2) The radiation protection personnel has the technical qualification as required by the Atomic Energy Act, the Radiation Protection Ordinance and the associated guidelines to perform its tasks.

2.2 (3) The radiation protection personnel is integrated in the plant organisation and equipped such that regarding the necessary precautions against damage caused by the construction and operation of the plant, it disposes of sufficient possible courses of action and the freedom to take decisions and has sufficient resources available to fulfil its functions. The radiation protection personnel is in particular not hindered from fulfilling its duties and will not be penalised for doing so.

2.2 (4) The radiation protection officer is authorised to report directly to the radiation protection supervisor and the plant manager.

2.2 (5) By his position within the organisation, the radiation protection officer is authorised to order the interruption of activities being performed if this is required to protect the personnel, the population or the environment from the hazards of ionising radiation and if no other serious reasons of a safety-related kind forbid such interruption.

2.3 Collective criteria for levels of defence 1 - 4

2.3 (1) The whole-body dose of persons staying within a controlled area is measured.

2.3 (2) Upon leaving a controlled area in which open radioactive sources are present, each individual is subjected to a contamination check and – if found to be contaminated – is decontaminated. If incorporation is suspected, the individual concerned is subjected to an incorporation measurement. If necessary, the personal and organ doses are determined and documented. If a controlled area has to be exited without passing through the contamination checkpoint, the contamination check has to be carried out later.

2.3 (3) The spreading of contamination through individuals and objects is counteracted by preventive measures (e.g. changing of protective clothing, monitoring of objects being taken out of controlled areas).

2.3 (4) The radiation protection officer defines the radiation protection measures in connection with the storage and handling of radioactive materials. Proper implementation of these measures is reviewed.

2.3.1 Planning, execution and follow-up of activities

2.3.1 (1) All activities in controlled areas are planned with participation of the radiation protection officer. The radiation protection personnel is involved in line with the planning.

2.3.1 (2) Work orders for tasks in controlled areas require examination and written consent by the radiation protection officer, who specifies the requisite radiation protection and monitoring measures regarding direct radiation, contamination, and incorporation. In the case of activities that are necessary to control or mitigate the consequences of event sequences and plant conditions on levels of defence 3 and 4, the radiation protection officer may forbear from giving his written consent prior to the work if the situation demands quick safety-oriented actions.

2.3.1 (3) The radiation protection officer defines criteria concerning the requirements of certain radiation protection measures according to subsection 2.3.1 (2), such as

- the use of radiation protection aids, like temporary shields and personal protective equipment,
- the use of remote-controlled working appliances,
- decontamination measures,
- measures to reduce stay time (e.g. practising the work on inactive models in the case of highly radioactive components).

2.3.1 (4) Regarding activities for which relevant individual and or collective doses are expected,

a) the radiation protection measures are assessed from a radiological point of view; if various different options exist, the radiation protection measures are balanced against each other, and the decision is explained in a comprehensible manner, taking into account the possible conflict between the objectives of the task and the radiation protection objectives;
b) the occurrence of disturbances and the removal or shielding of radiation sources is taken into consideration.

2.3.1 (5) Dose-intensive work on components is automated as far as achievable, taking into account all circumstances of individual cases.

Difficult dose-intensive work on components is tried out and practiced in advance, if necessary on models of the components, if this can help achieve a relevant reduction of radiation exposure.

2.3.1 (6) Regarding activities in areas with relevant local dose rates, the individual and collective doses expected during their performance are estimated when the activities are planned.

2.3.1 (7) Regarding activities for which relevant radiation exposure is expected, the radiation protection officer prepares a plan of the task-related recording of the individual doses of the personnel tasked with the activities.

2.3.1 (8) Prior to taking up a task in a controlled area, the individuals involved are instructed about the radiological situation at their respective workplaces as well as about the corresponding radiation protection measures to be taken.

2.3.1 (9) A task in a controlled area is not taken up until the radiation protection officer has given his permission within the framework of the internal regulations.

2.3.1 (10) The radiation protection officer takes care that the defined radiation protection measures are observed when performing activities in controlled areas. If need be, the radiation protection personnel provides support from a radiation protection point of view when the tasks are performed at the workplace and reviews the compliance with the radiation protection measures.

2.3.1 (11) Regarding activities for which relevant radiation exposure is expected, the radiation protection measures and the results of dose monitoring are documented. During and after the work, the results of dose monitoring are compared with the estimated planning levels according to subsection 2.3.1 (6).

2.4 Criteria for levels of defence 1 and 2

2.4 (1) Entry into and exit from a restricted access-area is on principle under supervision by the radiation protection officer or by other competent personnel acting on his behalf or by appropriately automated methods. Exceptions (e.g. in the event of an alert) are specified in the operating regimes.

2.4 (2) The radiation protection officer makes sure that access to an exclusion area is only allowed for planned operational processes or for urgent operational reasons. An exclusion area is only entered under the supervision of – and, if necessary, accompanied by – the radiation protection officer or a competent person acting on his behalf.

2.4 (3) Areas in which there is a risk of contamination being carried off are decontaminated, taking into account all circumstances of individual cases; until their decontamination, they are sealed off and marked as contamination zones by the radiation protection personnel in a way that is clearly visible and long-lasting.

2.4 (4) If surface contamination due to operational processes cannot be avoided in certain areas of work, non-fixed surface contamination is reduced to a level that is a low as achievable, taking into account all circumstances of individual cases, and measures are taken to protect the personnel.

2.4 (5) Relevant results and findings from radiation monitoring in connection with routine measurements, maintenance and modifications are documented and kept at a central location accessible at any time to the radiation protection officer or competent persons acting on his behalf. The kind, scope and statutory periods of safe keeping of these documents are specified according to the relevant rules and regulations.

2.4 (6) Regarding recurring activities in controlled areas, structural and technical installations as well as suitable working methods are provided to reduce the dose received by the personnel involved and to avoid any unnecessary radiation exposure. The radiation protection measures specified for the recurring activities are regularly checked for their effectiveness and expediency.

2.4 (7) At the beginning of a calendar year, the radiation protection officer prepares and assesses a survey of the individual and collective doses of the past year for the individual dose-intensive tasks. He examines in particular those cases in which individual doses or collective doses deviate clearly from the planning levels.

2.5 Criteria for levels of defence 3 and 4

2.5 (1) All activities to control, mitigate or eliminate the effects of event sequences and plant conditions on levels of defence 3 and 4 are planned with participation of the radiation protection officer. The radiation protection personnel is involved in the performance of the activities.

2.5 (2) The tasks of the radiation protection personnel with respect to the use of personnel planned in advance as well as to the pre-planned measures for the protection of the personnel possibly affected in the case of event sequences and plant conditions on levels of defence 3 and 4 are laid down in writing. These specifications also contain details on the scope and frequency of exercises for the radiation protection personnel.

3 Control of activity inventory and activity flow

3 (1) Design and operation of the plant are planned such that the amount and activity of the radioactive waste as well as of radioactive materials to be utilised without detrimental effects is kept as low achievable, taking into account all circumstances of individual cases.

3.1 Levels of defence 1 and 2

3.1 (1) For compliance with the safety objectives according to Section 2.4 (1) of the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1) for levels of defence 1 and 2, the sources of ionising radiation related to the operation of the plant are identified at the plant design stage and kept under control during plant operation by special measures and installations in line with the requirements of the Radiation Protection Ordinance.

3.1 (2) The entry of activated corrosion products or those that can be activated into the reactor coolant is kept as low as achievable, taking into account all circumstances of individual cases, by the choice of materials as well as by the chemical conditioning mode of the coolant.
N o t e: In connection with the choice of materials it is in particular possible to achieve a relevant reduction of the local dose rate by minimising cobalt content and avoiding the use of cobalt-based alloys.

3.1 (3) Any entry of nuclear fuel and fission products as well as of oxide film spallings stemming from fuel cladding tubes into the coolant is kept as low as achievable, taking into account all circumstances of individual cases, by quality assurance measures upon the manufacture and handling of the fuel elements as well as by the mode of operation.

3.1 (4) Measures and installations are provided by which fuel rod defects can be detected. If the decision is taken to continue operation of the plant with defective fuel rods, the resulting radiation exposure of the operating and maintenance personnel during plant operation as well as in connection with the next refuellings is taken into account.

3.1 (5) Purification systems for the reactor coolant system and for the spent-fuel pool are installed which are operated on demand and which are effective for both dissolved and undissolved impurities.

3.1 (6) Systems containing radioactively contaminated media are sealed such that the spreading of radioactive materials is prevented. The effectiveness of barriers and retaining functions is monitored. For this purpose, values for maximum permissible leakages are defined in dependence of the respective system and of the respective medium.

3.1 (7) Any entry and carry-off of activity into connected non-activity-bearing supply systems (e.g. auxiliary steam system, demineralised-water system, rinse and seal water systems) is reliably avoided by precautions (e.g. by the installation of valves, the layout of pipe connections, pressure differences).

3.1 (8) Radioactively contaminated waters (e.g. coolant system, sump, laboratory or rinse waters) are collected, treated and processed by their origin. If any further use of the waters is out of the question, they are released under control.

3.1 (9) Radioactively contaminated exhaust gases from nuclear systems are principally collected and treated according to their contamination by activity retention units or delay. For the delay, delay periods that are observed are such that the release of short-lived radioactive noble gases will not contribute relevantly to radiation exposure.

3.1 (10) The collection, handling, storage and treatment of radioactive waste and radioactive materials to be utilised without detrimental effects is devised such that the contamination and radiation exposure of the personnel is avoided as far as achievable, taking into account all circumstances of individual cases. This is taken into account in the preparation of a residual materials and waste concept.

3.1 (11) Radioactive waste and radioactive materials to be utilised without detrimental effects are principally collected and stored separately according to the further handling provided for them. Exceptions are justified.

In particular, materials which are intended for clearance or have been cleared according to the provisions of the Radiation Protection Ordinance, are collected and stored separately from other radioactive materials to prevent contaminations.

3.2 Level of defence 3

3.2 (1) For compliance with the safety objectives according to Section 2.4 (1) of the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1) for level of defence 3, the potential sources of ionising radiation that may originate from events on level of defence 3 are identified in the design of the plant and measures and installations provided to keep these sources under control.

3.2 (2) Radioactively contaminated waters that may arise from events on level of defence 3 are collected within the plant. Corresponding measures are provided and installations exist. Waters released within the containment, e.g. as a result of loss-of-coolant accidents, are if achievable retained within the containment and within the systems necessary for core cooling until further treatment. The necessary processing and release in the long-term phase is carried out according to a concept that considers the radiological aspects.

N o t e: According to Section 5, sampling and monitoring systems are provided which make it possible to obtain sufficient information, even under the conditions of events on level of defence 3, on

- the dose rate (according to Section 5.5.2),
- the activity concentration in room areas (according to Section 5.4.2) as well as on
- the activity concentration in systems and the effectiveness of barriers

(according to Section 5.3.2).

3.3 Level of defence 4

N o t e: Criteria for monitoring and sampling to keep the activity flow on level of defence 4 under control are contained in Section 5.3 and 5.4.

4 Structural and technical radiation protection

4 (1) Structural radiation protection (e.g. components of building structures) is aimed at the safe confinement of radioactive materials, the shielding of radiation sources, and the prevention

of the spreading of radioactive materials through the plant. The design and layout of rooms with a view to an optimisation of stay times are also part of structural radiation protection.

4 (2) Technical radiation protection comprises
- the use of facilities (i.a. systems, tools, and methods) as well as
- further provisions of a material kind, such as choice of material and decontaminability

to fulfil the criteria according to subsection 1 (1).

4.1 General criteria

4.1.1 Levels of defence 1 and 2

4.1.1 (1) When planning structural and technical radiation protection installations, an increase in the local dose rate of accessible areas due to long-time operation of the plant is taken into account.

4.1.1 (2) The structural design of the plant and the design and layout especially of activity-retaining components takes into account that their replacement may become necessary during the operating period of a nuclear power plant. Therefore provisions exist that ensure that components can be replaced without having to be disassembled and with as little radiation exposure of the personnel as achievable to reduce the radiation exposure, taking into account all circumstances of individual cases. The measures and installations necessary for fulfilling these requirements are not in conflict with any safety-related requirements; for example, the possibility of carrying out in-service inspections on these components is not restricted.

4.1.1 (3) The rooms of the controlled area are classified and correspondingly shielded according to their intended use and the frequency of the stay times of individuals.

4.1.1 (4) The walls, ceilings and floors of rooms housing radiation sources are dimensioned such that the local dose rate brought about by radiation entering from neighbouring rooms will only contribute a small proportion of the upper local dose rate reference value applying to the room concerned.

4.1.1 (5) For often frequented rooms such as corridors, staircases, the hygiene tract, and first-aid rooms or for workplaces that are often manned, it is ensured by shielding or by providing enough space to keep a distance that a stay in these areas will not lead to a relevant radiation exposure of the personnel.

4.1.1 (6) The space required for the unhindered performance of maintenance, to set up additional shields, to use special tools or other removal aids and to set down removed parts is included in the planning. The loads that occur are considered in the rating of the load-bearing capacity of the floors.

4.1.1 (7) Rooms, systems and components within the permanent controlled area as well as the floor of the part of the hygiene tract that is located outside the controlled area are easy to decontaminate.

4.1.1 (8) The measures and installations necessary for radiation protection (measuring instruments, protective equipment, preparations, sampling systems, radiation protection aids, etc.), rooms for the preparation, performance and evaluation of measurements, spaces for the calibration of mobile radiation measuring instruments and spaces for radiation protection aids as well as test emitters and samples are available in sufficient quantities and with the requisite quality.

4.1.1 (9) Component and system sections in which non-fixed depositing of radioactive materials cannot be avoided can be rinsed in order to wash off these materials. Components or system sections containing liquid radioactive materials can be drained completely, as far as technically feasible.

4.1.1 (10) The installations, rooms and storage facilities necessary for the decontamination of removed parts and components are available. A "hot workshop" is provided for the processing of activated and contaminated components and component parts.

4.1.1 (11) Components in areas of high local dose rates are designed and installed such that they require particularly little maintenance and that such maintenance can be easily performed.

4.1.1 (12) Components producing a high dose rate are principally shielded from each other by being installed in separate rooms. Exceptions are justified.

4.1.1 (13) Components that are expected to require in-service inspections and maintenance work frequently are arranged in the room such that any unnecessary radiation exposure is avoided when they are accessed and the work can be performed under ergonomically favourable conditions. If necessary, removal aids for heavy components are available. For the reduction of the radiation exposure of the personnel, provisions are made to minimise stay time within the radiation field (e.g. automation, remote control, quickly detachable insulation).

4.1.1 (14) The planning of the layout of components considers that regular access to a component with a relevant dose rate is principally not via areas in which the dose rate is higher than that of the component itself. Exceptions are justified.

4.1.2 Level of defence 3

4.1.2 (1) If installations need to be operated to control events on level of defence 3, it is ensured that access to these installations is as unhindered as achievable. When planning the measure, the requirements of the Radiation Protection Ordinance regarding the limitation of occupational radiation exposure are used as a basis for the calculation of the entire expected radiation exposure of the measure, including the way to and from the place of installation.

4.1.2 (2) Regarding installations which are expected to require maintenance or repair within the framework of the long-term control of events on level of defence 3, measures and installations are provided for shielding, should the need for such maintenance arise. There is enough space available to bring in necessary removal aids, or such aids are already locally installed.

4.1.2 (3) Areas are provided within the plant's grounds that are suitable for gathering the personnel as well as for measuring their contamination in the case of an event on level of defence 3. These areas are sufficiently protected for this purpose against any increased radiation exposure and contamination.

4.1.3 Level of defence 4

4.1.3 (1) All installations are arranged and if necessary shielded such that the possibility to carry out any manual actions provided in connection with the measures on level of defence 4 is ensured.

4.1.3 (2) Areas are provided within the plant's grounds that are suitable for gathering the personnel as well as for measuring their contamination in the case of event sequences and plant conditions on level of defence 4. These areas are sufficiently protected for this purpose against any increased radiation exposure and contamination.

4.1.3 (3) Areas are provided within the plant which in the case of event sequences and plant conditions on level of defence 4 are suitable for accommodating the members of the plant-internal emergency organisation tasked with coping with the emergency situation.

4.2 Ventilation systems

4.2 (1) The nuclear power plant is equipped with reliable ventilation systems for the following rooms:

a) rooms in which it cannot be ensured without ventilation systems that the amount of radioactive materials to be released into the environment with the extracted air is kept low to fulfil the relevant criteria according to subsection 2.4 (1) of the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1);
b) rooms in which the activity concentration in the room air has to be kept low for reasons of occupational radiological protection and this cannot be ensured without ventilation systems.

N o t e: Further safety criteria for ventilation systems are dealt with in the "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components" (Module 10).

4.2 (2) If the concentration of radioactive materials in the air of certain rooms may rise to beyond corresponding limits that are permissible regarding the discharge of radioactive materials with exhaust air, the associated ventilation systems are fitted with air filter systems. It is permissible to realise ventilation systems such that the exhaust air is guided via the filters. The air filter systems are sufficiently reliable and conditioned such that they will guarantee the requisite retention efficiency under the respective conditions of operation. The necessary equipment is provided for the verification of their specified condition.

4.2.1 Levels of defence 1 and 2

4.2.1 (1) The ventilation systems are designed and conditioned and brought into tune with the features of the other installations such that on levels of defence 1 and 2, the permissible values for the activity concentration in the room air and for the discharge of radioactive materials are not exceeded. Air recirculation systems are suitably combined with exhaust air systems so that the relevant criteria according to subsection 2.4 (1) of the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1) are fulfilled. Exhaust air systems executing functions for maintaining subatmospheric pressure during events on level of defence 2 are connected to the emergency power supply system.

4.2.1 (2) In rooms that are connected to the ventilation systems, any uncontrolled release of activity into the environment is prevented by maintaining subatmospheric pressure and by correspondingly guided flows or by the closing of suitable isolating flaps. The actions required to do this can be operated from the control room.

4.2.1 (3) To prevent radioactive materials from being carried off through the room air, the air in the restricted access areas is on levels of defence 1 and 2 on principle guided in such a way and the groups of rooms are on principle sealed off from each other and from the atmosphere such that the air from rooms or groups of rooms at a lower risk of contamination is guided to rooms or groups of rooms at a higher risk of contamination. Exceptions are justified.

4.2.1 (4) The extracted air is monitored and released via filters if necessary. Any extracted air volumes extracted on levels of defence 1 and 2 from containment areas housing reactor coolant-carrying components for the purpose of maintaining subatmospheric pressure are continuously cleaned by means of aerosol and iodine sorption filters.

4.2.2 Level of defence 3

4.2.2 (1) The ventilation systems are designed and conditioned and brought into tune with the features of the other installations such that on level of defence 3, the permissible values for the activity concentration in the room and for the discharge or possible release of radioactive materials are not exceeded. Air recirculation systems are suitably combined with exhaust air systems so that the relevant criteria according to subsection 2.4 (1) of the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1) are fulfilled. Exhaust air systems intended for use during or after events on level of defence 3 are connected to the emergency power supply system.

4.2.2 (2) Measures and installations are provided to prevent the escape of high levels of activity from the containment. If the containment is ventilated in closed condition, an automatic sealing device is available that will respond if high levels of activity occur in the containment.

4.2.2 (3) Filter systems intended for use during or after events on level of defence 3 for cleaning the exhaust air and thereby to limit the consequences of the event are designed such

that there will be no deviations below the following separation efficiency limits when used on level of defence 3:
- suspended matter: η= 99.9%
- organically bound iodine: η= 99%
- elementary iodine: η=99.99%.

4.2.2 (4) Filter systems that are constantly or temporarily impinged with exhaust air on levels of defence 1 and 2 and which have to be used during or after events on level of defence 3 are installed and operated such that any deviation below the minimum separation efficiency limit defined as the basis for planning technical protection measures against events on level of defence 3 is excluded.

In particular, the loading with contaminants during the use on levels of defence 1 and 2 is monitored, and a sufficient margin to the minimum separation efficiency is ensured by the timely replacement of the filter material.

4.2.2 (5) Regarding their active components (ventilator and secondary heater), filter systems according to subsection 4.2.2 (3) are designed with a 3 x 100% or 4 x 50% redundancy and regarding their passive components with a 2 x 100% redundancy (to be either added or switched over). The filter systems are equipped with moisture separators and secondary heaters or with technically equivalent installations to prevent the filter inlet air conditions from falling below dew point and to avoid condensate accumulation, or else to limit these phenomena to an extent that has been shown not to fall short of the required separation efficiency levels. The conditions occurring in the filter inlet air during or after an event on level of defence 3 are specified. If redundant filters are housed in the same room, it is ensured that
a) the redundant filters cannot fail simultaneously due to an event on level of defence 3 which to control they are needed for
b) a redundant filter system cannot be caused to fail as well by another filter system in connection with an event on level of defence 3 which to control it is needed for.

4.2.3 Level of defence 4

4.2.3 (1) Ventilation systems that are intended for use within the framework of measures provided on level of defence 4 are conditioned such that they fulfil the safety-related functions required for this purpose.

4.2.3 (2) Filter systems intended to be used for filtered containment venting during plant conditions on level of defence 4c are designed such that there will be no deviations below the following separation efficiency limits:
f) suspended matter: η= 99.9%
g) elementary iodine: η = 90%

The operability of the filter systems for the representative event sequences and phenomena considered according to Section 2 of the "Safety Criteria for Nuclear Power Plants: Criteria for Accident Management" (Module 7) is ensured.

4.3 Waste water treatment systems

4.3.1 Levels of defence 1 and 2

4.3.1 (1) The installations for waste water treatment and their storage capacity are designed such that the water accumulating during operation on levels of defence 1 and 2 in areas with open radioactive materials can be collected and, if necessary, treated.

4.3.1 (2) It is ensured by reliable measures and installations that any radioactively contaminated water can neither reach into the soil and therefore possibly into the groundwater nor into any non-reactivity-retaining system or the surface water.

4.3.2 Level of defence 3

4.3.2 (1) Measures and installations are provided to prevent any radioactively contaminated water arising due to an event on level of defence 3 from reaching uncontrolled into the environment of the plant.

4.3.3 Level of defence 4

N o t e: The fundamental criteria according to subsection 4.1.3 (1) apply.

4.4 Other systems containing an activity inventory

4.4.1 Levels of defence 1 and 2

4.4.1 (1) Activity-retaining systems are vented under control; any systems in which relevant accumulations of fission and radiolysis gases may occur are connected to the exhaust gas system. The other systems are connected to the exhaust air system.

4.4.1 (2) Installations for pressure limitation in systems containing contaminated media and the receiving systems or room areas are conditioned such that upon response, the media escaped into the receiving systems or room areas can be discharged under control.

4.4.2 Levels of defence 3 and 4

N o t e: The general criteria according to subsection 4.1.2 (1) and (2) apply to level of defence 3 and those according to subsection 4.1.3 (1) to level of defence 4.

5 Radiation and activity monitoring within the plant

N o t e: For radiation and activity monitoring equipment executing functions of the accident instrumentation, further criteria ensue from the "Safety Criteria for Nuclear Power Plants: Criteria for Instrumentation and Control and Accident Instrumentation" (Module 5), "Safety Criteria for Nuclear Power Plants: Criteria for Electric Power Supply" (Module 12).

5 (1) The following is provided for radiation and activity monitoring within the plant:
1. installations for the monitoring of radioactive materials that may be discharged or released either airborne or with waste water;
2. stationary installations for measuring the concentration of radioactive materials in circuits in which corresponding monitoring is necessary for the early detection of any released radioactive materials;
3. stationary installations for measuring the concentration of radioactive materials in the room air of groups of rooms or rooms in which corresponding monitoring is necessary to protect personnel or to detect any released radioactive materials in good time;
4. stationary installations for measuring local dose rates;
5. installations for measuring personal doses, the local dose rate, the room air concentration in workplaces and the contamination of individuals and objects;
6. adequate laboratory facilities for evaluating and analysing radioactive samples.

5.1 Monitoring of the discharge or release of airborne radioactive materials into the environment

5.1 (1) Measures and installations are provided for the monitoring of the discharge of airborne radioactive materials as well as for any release of airborne radioactive materials.

5.1 (2) Monitored are discharges and releases of radioactive materials via the stack as well as via all other paths on which airborne radioactive materials may be discharged or released in relevant amounts.

5.1 (3) The monitoring equipment components to be permanently operated dispose of a reliable power supply supply.

5.1.1 Monitoring during operating conditions on levels of defence 1 and 2

5.1.1 (1) The discharge of airborne radioactive materials with the exhaust air is monitored by stationary installations. Verification is provided with the help of these installations that the licensed limits for activity releases are adhered to and that the dose limits applying to individuals in the surrounding environment are not exceeded. The measured values are recorded.

5.1.1 (2) For this purpose,

a) any releases of radioactive noble gases, radioactive suspended matter and radioactive iodine with the exhaust air are monitored by continuous measurement and assessed in detail
b) any discharges of tritium, radioactive strontium, alpha emitters and carbon-14 with the exhaust air are assessed in detail.

5.1.1 (3) The exhaust air according to subsection 4.4.1 (1) is monitored.

5.1.1 (4) The installations for monitoring the discharge of radioactive noble gases and for the detailed assessment of the discharge of radioactive suspended matter and radioactive iodine with the vent stack air are designed redundant.

5.1.2 Monitoring of events on level of defence 3

5.1.2 (1) The monitoring of the discharge of airborne radioactive materials with exhaust air is ensured even for events on level of defence 3.

5.1.2 (2) To determine the activity of airborne radioactive materials in the vent stack air in events on level of defence 3, suitable stationary collecting and measuring devices are available for radioactive noble gases, radioactive suspended matter and gaseous radioactive iodine.

5.1.2 (3) If in events on level of defence 3 any airborne radioactive materials in radiologically relevant amounts may be released via paths of which the exhaust air flow is not monitored, the specific activity or activity concentration of the medium in the system concerned and the amount of medium discharged are determined to monitor the release, and the ensuing activity release is calculated.

5.1.3 Monitoring during event sequences and plant conditions on level of defence 4

5.1.3 (1) It is ensured that the release of airborne radioactive materials in connection with event sequences and plant conditions on level of defence 4 can be estimated.

5.1.3 (2) To estimate the release via the filtered containment venting system during plant conditions on level of defence 4c, suitable collecting and measuring devices are available for radioactive noble gases, radioactive suspended matter and gaseous radioactive iodine.

5.1.3 (3) High-dose-rate measuring devices and sampling systems are available which during plant conditions on level of defence 4c allow an estimate of the airborne activity in the containment to be able to make a prediction of the extent of the activity released from the containment in case of planned filtered venting or potential danger to the integrity of the containment.

5.1.3 (4) For event sequences and plant conditions on level of defence 4 in which the release of airborne radioactive materials into the environment cannot be otherwise determined, the possibility to estimate the release with the help of the measuring results of immission monitoring is ensured according to Section 6.1 in conjunction with the recording of dispersion conditions according to Section 6.2.

5.2 Monitoring of the discharge of radioactive materials into the environment with water

5.2.1 Monitoring in connection with operating conditions on levels of defence 1 and 2 as well as during events on level of defence 3

5.2.1 (1) The discharge of radioactive materials with water is monitored; the data acquired from monitoring are used to verify that the licensed values for the discharge are not exceeded.

5.2.1 (2) Any discharge of radioactive materials with the waste water from controlled areas is monitored and assessed in detail.

N o t e: According to subsection 3.1 (8) and 3.2 (2), the waste waters from controlled areas are collected for all operating conditions on levels of defence 1 and 2 as well as for all events on level of defence 3 and will only be discharged under control if it is ensured that specified activity concentration limits in the transfer vessel are not exceeded.

5.2.1 (3) The discharge of waste water from controlled areas is monitored by means of stationary activity measuring points and is automatically interrupted in good time if specified limits are exceeded.

5.2.1 (4) The discharge of radioactive materials via other systems that may retain activity, e.g. nuclear service water or turbine building waste water, is monitored and assessed in detail if specified activity limits are exceeded.

5.2.1 (5) The water returning into the receiving water is continuously monitored.

5.2.2 Monitoring during event sequences and plant conditions on level of defence 4

5.2.2 (1) During event sequences and plant conditions on level of defence 4, any releases via the waste water path are estimated.

5.3 Monitoring of systems

5.3 (1) Measures and installations are provided by which the activity flow within the plant and the effectiveness of barriers against the escape of radioactive materials is monitored to allow the early detection of a threatening release or inadmissible spreading of radioactive materials in the plant and to make it possible that any necessary measures are taken in time.

5.3.1 Monitoring of operating conditions on levels of defence 1 and 2

5.3.1 (1) Monitoring is designed such that any inadmissible changes in the activity concentration in systems – especially activity passover into systems or system areas that, according to their design, do not contain radioactive materials – are reliably detected.

5.3.1 (2) The activity concentration is continuously monitored by means of stationary measuring devices and by regular sampling. If the activity concentration in the reactor coolant system, in the systems directly connected to it or in the spent-fuel pool cooling and clean-up systems is not continuously monitored but determined by sampling, samples are taken at sufficient intervals.

5.3.1 (3) If defined thresholds are exceeded in the case of the continuously measuring installations, an alarm signal is triggered in the control room.

5.3.1 (4) Determination of the activity concentration in the systems is also done by sampling if there are any indications of an increased activity concentration.

5.3.2 Monitoring during event sequences on levels of defence 3 to 4b

5.3.2 (1) Monitoring is designed such that the entry of radioactive materials due to event sequences on levels of defence 3 to 4b into systems that, according to their design, do not contain radioactive materials is detected so that the necessary measures to limit a corresponding possible release can be initiated and that if need be, the information necessary for the initiation of emergency measures and for providing support in connection with any disaster control measures is available.

5.3.2 (2) Regarding systems which according to subsection 5.3.1 (2) are monitored by continuous measuring, this is also ensured on level of defence 3.

5.4 Monitoring of radioactivity in the room air (stationary system)

5.4 (1) Rooms or groups of rooms of the controlled area that are frequently accessed by operating personnel and in which increased levels of room air concentration may occur are continuously monitored for the radionuclide groups that (noble gases, suspended matter, gaseous iodine) that may occur. For this purpose, stationary monitoring devices are installed which trigger warning signals if thresholds are exceeded.

The stationary system gives information as to the walkability of monitored areas, the plant condition, and the integrity of the systems.
N o t e: In addition, mobile measuring devices according to Section 5.6 are available.

5.4.1 Monitoring in connection with operating conditions on levels of defence 1 and 2

5.4.1 (1) The system is designed such that in connection with operating conditions on levels of defence 1 and 2
a) any increased activity concentrations in the room air are detected,
b) the buildings or groups of rooms affected can be identified, and
c) leaks in activity-retaining systems are detected (leakage monitoring).

5.4.2 Monitoring event sequences and plant conditions on levels of defence 3 and 4

5.4.2 (1) The system is designed such that during events on level of defence 3, any activity release into the room air can be detected and confined to certain areas.

5.4.2 (2) To monitor the activity in the containment atmosphere during event sequences and plant conditions on levels of defence 3 and 4, high-dose-rate monitoring devices and sampling systems are available, providing the information necessary for the initiation of emergency measures and for providing support in connection with any disaster control measures.
N o t e: The accident management measures for taking samples for the diagnosis of the condition in the containment are implemented that provide information that is taken into account in the assessment of the radiological consequences of filtered containment venting (see "Safety Criteria for Nuclear Power Plants: Criteria for Accident Management" [Module 7], in subsection 3.1 (2) and 3.3 (6)).

5.5 Monitoring of the local dose rate (stationary system)

5.5 (1) For the continuous monitoring of local dose rates in the controlled areas, a stationary system is available which triggers warning signals if thresholds are exceeded.
N o t e: In addition, mobile measuring devices according to Section 5.6 are available.

5.5 (2) The values measured by this stationary system are indicated on site and in the control room and are recorded. The values measured are monitored for any deviations above warning thresholds. Any such deviation is signalled on site and in the control room both visually and acoustically.

5.5.1 Monitoring in connection with operating conditions on levels of defence 1 and 2

5.5.1 (1) Stationary dose rate measuring devices of this system are installed in areas of the plant in which changes in the local dose rate are expected and where individuals have to be warned.

5.5.2 Monitoring in connection with events on level of defence 3

5.5.2 (1) The system is designed such that in events on level of defence 3 it can provide information about the walkability of monitored areas.

5.5.2 (2) To assess the radiological consequences of events on level of defence 3, local dose rates are monitored in suitable locations within the plant (e.g. in the reactor building and in the case of boiling water reactors also in the turbine building).

5.5.3 Monitoring during event sequences and plant conditions on level of defence 4

5.5.3 (1) To assess the radiological consequences of event sequences and plant conditions on levels of defence 4b and 4c, local dose rates are monitored in suitable locations within the plant (e.g. in the reactor building and in the case of boiling water reactors also in the turbine building) so that the information necessary for the initiation of emergency measures and for providing support in connection with any disaster control measures is provided.

5.6 Monitoring of workplaces and other measuring and monitoring tasks

5.6 (1) Regarding individuals carrying out tasks in a controlled area, provisions aimed at the protection of these individuals exist to monitor their workplaces, to carry out further monitoring measures, e.g. at access points and personnel airlocks as well as on inspection rounds, and to allow the determination of their body doses according to the regulatory requirements.

5.6 (2) Provisions exist that such necessary measurements and controls can be carried out
a) upon taking moveable objects out of controlled or supervised areas according to the provisions of the Radiation Protection Ordinance,
b) in connection with clearance procedures according to the provisions of the Radiation Protection Ordinance, and
c) on radioactive waste and materials to be utilised without detrimental effects with regard to their characterisation and transportability and the integrity of waste packages.

5.6.1 Monitoring during operating conditions on levels of defence 1 and 2

5.6.1 (1) For the measuring tasks according to subsection 5.6 (1), mobile measuring devices or installations are provided in suitable locations so that samples can be taken and evaluated:
a) dose rate measuring devices for
aa) gamma and beta radiation,
ab) neutron radiation,
b) installations for the nuclide-specific recording of contamination, e.g. by sampling and evaluation of the samples in the laboratory,
c) measuring devices for the determination of surface contamination,
d) equipment for the determination of the activity concentration in the room air.

5.6.1 (2) Regarding the monitoring of workplaces provided for regular stay over a longer period of time and where rapidly changing radiological conditions might prevail, stationary measuring devices are available wherever necessary for measuring local dose rates and activity concentrations in the room air for monitoring during operating conditions on levels of defence 1 and 2.

5.6.1 (3) The following equipment is provided for monitoring individuals carrying out tasks in the controlled area:
a) dose warning devices,
b) personal dosimeters,
c) personal contamination monitors,
d) measuring devices for determining incorporated activity.

5.6.1 (4) For the measuring tasks according to subsection 5.6 (2), corresponding measuring places are provided in suitable locations within the plant, and sufficient mobile measuring devices are available.

5.6.2 Monitoring during event sequences and plant conditions on levels of defence 3 and 4

5.6.2 (1) Regarding the design of measures for events on level of defence 3 and the planning of measures for event sequences and plant conditions on level of defence 4, it is ensured that these measures can be carried out under adequate radiation protection monitoring. This includes in particular the provision of suitable measuring devices.

5.7 Documentation of the results of radiation and activity monitoring within the plant

5.7 (1) The results of the measurements according to Section 5.1 to 5.6 are documented and kept in line with the relevant legal and regulatory stipulations as well as according to the requirements of the relevant safety codes and guides. If the keeping of samples is required for purposes of preserving evidence, suitable provisions are made.

5.7 (2) If a routine is established in line with the legal stipulations under which the results have to be reported to the competent authority in case of any deviations above specified limits or on special occasions, the requirements of the relevant safety codes and guides and of regulatory guidelines regarding the scope and structure of such reports are fulfilled.

6 Radiation monitoring in the environment

6 (1) In addition to emission monitoring, immission monitoring allows the additional control of the discharge of radioactive materials as well as of the adherence to dose limits in the environment of the plant. Corresponding facilities and measuring programmes are provided.

6 (2) There exist two programmes for immission monitoring:
a) one programme that is carried out by the licensee (especially for monitoring the vicinity as well as primary media), and
b) a supplementary and controlling programme that is carried out by an independent measuring organisation (referred to in the following as independent measuring agency) (especially for monitoring the surrounding area further afield as well as foodstuffs and drinking water).

For reasons of verification and for comparison, selected media are monitored by both programmes.

6 (3) The sampling and measuring locations are situated in places where a relevant dose contribution is expected due to the dispersion of the emitted radioactive materials through the environment, taking into consideration the actual use of these places by humans or animals staying there and the actual consumption of foodstuffs produced there. Furthermore, sampling and measuring locations are provided that are largely uninfluenced by the plant's specified normal operation (reference locations).
N o t e: The Precautionary Radiation Protection Act regulates measures for monitoring environmental radioactivity that serve for the determination of radioactivity levels and dose rates throughout wide areas. These measures do not refer to the monitoring of a concrete plant.

6.1 Immission monitoring

6.1.1 Immission monitoring regarding levels of defence 1 and 2

6.1.1 (1) For immission monitoring on levels of defence 1 and 2, installations are provided for the determination of
a) local doses, local dose rates, and
b) activity concentrations in ambient air, soil, vegetation, foodstuffs, waters, and precipitation.

6.1.1 (2) The measuring programmes are designed such that any possible long-term changes resulting from the discharge of radioactive materials can be shown in the locations relevant in connection with the different exposure paths. For this purpose, the results of the measuring programme carried out prior to first commissioning – by which the environmental radioactivity and dose rates so far uninfluenced by the operation of the plant were recorded - are consulted.

6.1.2 Immission monitoring regarding levels of defence 3 and 4

6.1.2 (1) For immission monitoring on levels of defence 3 and 4, installations are provided for the determination of
a) local doses, local dose rates,
b) soil contamination, and
c) activity concentrations in ambient air, soil, vegetation, foodstuffs, waters, and precipitation.

6.1.2 (2) For immission monitoring on levels of defence 3 and 4, sampling and measuring methods exist. The necessary measurements are practiced by regular measuring runs by the licensee and the independent measuring agencies at defined sampling and measuring points of the accident measuring programme.

6.1.2 (3) For levels of defence 3 and 4, sampling and measuring methods are defined whose measuring ranges link up seamlessly with the measuring ranges for specified normal operation and which reach far enough to cover the immissions associated with all events postulated on level of defence 3 as well as those on level of defence 4 that require disaster control measures.

6.2 Recording of dispersion conditions

6.2 (1) To assess the radiological consequences of emissions on levels of defence 1 to 4, the meteorological and hydrological parameters relevant in connection with the dispersion and depositing of radioactive materials are recorded site-specifically.

6.2 (2) Using instrumentation at the plant site, the influencing variables relevant in connection with the dispersion of radioactive materials are continuously measured.

6.2 (3) In case of any instrumentation unavailabilities, substitute measures are in place.

6.3 Documentation of the results of environmental monitoring

6.3 (1) The licensee and the independent measuring agencies report to the competent authorities about the results of immission monitoring in the form of quarterly and annual reports. Irrespective of these reports, the competent authorities are informed without delay if the measuring results raise concerns that dose limits for members of the population may be exceeded.

7 Determination of radiological consequences for the planning of disaster control measures

N o t e: In this section, criteria are defined for the determination of radiological consequences for the planning of disaster control measures by means of deterministic analyses. As soon as detailed bases of calculation are available in this respect, these will be applied.

7 (1) For the planning of disaster control measures, the potential radiological consequences in the vicinity of the plant are determined for the plant conditions, event sequences and phenomena (levels of defence 4b and 4c) - which involve radioactive releases that may require disaster control measures – that are considered in the planning of accident management measures according to Section 2 of the "Safety Criteria for Nuclear Power Plants: Criteria for Accident Management" (Module 7).

7 (2) The aim of the determination of the radiological consequences is to allow an estimation of the potential need for the disaster control measures
a) sheltering,
b) iodine prophylaxis,
c) evacuation.

For this purpose, values that are as realistic as achievable are determined for the above-mentioned measures to be compared with the respective intervention levels.

7 (3) For the determination of the radiological consequences, assumptions, models and parameters are used that are as realistic as achievable. Wherever this is not practicable, any uncertainties in the knowledge on the relevant processes and parameters are considered by conservative assumptions that are commensurate with the objectives according to subsection 7 (2).

7.1 Determination of source terms

7.1 (1) On level of defence 4b, source terms are estimated for leak events with containment bypass on the basis of the extent of the event-induced fuel rod cladding failure to be postulated.

7.1 (2) Determination of the source term for plant conditions on level of defence 4c is done plant-specifically on the basis of release categories, appropriately summarising plant conditions with similar releases and release patterns.

7.2 Determination of the radiological consequences

7.2 (1) The radiological consequences are determined specifically - with consideration of the variation of the dispersion conditions - for the individual zones and sectors into which the surrounding environment of the plant is divided for disaster control planning.

7.2 (2) The radiological consequences are estimated regarding the dispersion conditions that are representative for the site. Here, the variability of the dispersion conditions is considered as far as it may lead to relevant differences of the radiological consequences with regard to disaster control planning.

7.2 (3) Radiation exposure is determined in such a manner that it allows a direct comparison with the relevant intervention levels for the disaster control measures mentioned in Section 7 (2). The calculation is based on exposure paths and times that are in line with the definition of the intervention levels.

Annex 1

Detailed criteria for the calculation of the radiological consequences for verifying the limitation of radiation exposure of the population on levels of defence 1 to 3

A1 1 Levels of defence 1 and 2

A1 1 (1) For planning purposes, assumptions, parameters and calculation models are used to calculate the exposure to direct radiation in the vicinity of the plant. These assumptions, parameters and calculation models yield a conservative result of the calculated radiation exposure.

A1 1 (2) For planning purposes, the general administrative provisions specifying the provisions of the Radiation Protection Ordinance apply to the calculation of the radiation exposure due to the release of radioactive materials during plant operation on levels of defence 1 and 2.

A1 2 Level of defence 3

A1 2 (1) The possible radiological consequences are calculated for those events on level of defence 3 for which fulfilment of the radiological safety objectives has to be verified according to the "Safety Criteria for Nuclear Power Plants: Events to be Considered in Pressurised and Boiling Water Reactors" (Module 3). The calculations are generally based on the assumptions, parameters and calculation models specified in the relevant Radiological Accident Calculation Bases.

A1 2 (2) Other parameters and calculation models may be used if this is justified by the design features of the nuclear power plant, the characteristics of the respective sites or the release and dispersion conditions. Any deviations from the Radiological Accident Calculation Bases are justified case by case, showing that the other parameters and calculation models correspond better to the actual conditions of the respective individual cases.

A1 2 (3) Assumptions, parameters and calculation models are used for the calculation with which the expected radiation exposure in the environment of the plant is determined in a manner that is sufficiently conservative for planning purposes.

A1 2 (4) For this purpose, substantiated assumptions concerning the initial conditions and characteristics of the plant (e.g. regarding activity content, leak rates, efficiency of purification and retention systems), the activity release into the enclosing systems, deposition processes on installed components and the time history of leak or blowdown rates for the enclosing systems as well as realistic assumptions, calculation models and parameters concerning the event sequence and the release and dispersion of radioactive materials are applied as a basis. If possible, frequency distributions that have been observed are also taken into account.

If simplified calculation methods are used, the assumptions, calculation models and parameters are defined such that an overall conservative result will be reached in accordance with subsection A1 2 (3).

Alternatively, if realistic assumptions, calculation models and parameters are applied, it has to be shown that at least 95% of the scatter range of the expected radiation exposure are covered, with quantification of the uncertainties. It is sufficient to show that at least 95% of the scatter range are covered also for interim results and partial stages of the analysis (e.g. for the calculation of the activity release a n d / o r the calculation of the dispersion of radioactive materials) if there is proof that an overall conservative result concerning the expected radiation exposure will be reached by the chosen combination of realistic and conservative partial stages of the analysis.

N o t e: For a safety demonstration including a quantification of the result uncertainties, the criteria according to the "Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation" (Module 6), Section 3.3, apply; for a conservative safety demonstration, the criteria of Section 3.4 apply.

A1 2 (5) The parameters for the calculation of the activity release, the values of which may disperse a great deal, are

– estimated conservatively, or

- chosen such that the nuclide-specific activity concentration and contamination in the environment of the plant to be calculated form the release cover at least 95% of the scatter ranges, or
- defined with consideration of the subsequently ensuing conditions by means of their observed frequency distributions.

A1 2 (5a) Verified distribution functions of the parameters are available; this also includes the acquisition of the measured values in a representative time-dependent distribution.

A1 2 (5b) The parameter values used for the calculation of the activity release cover 95% of the distribution of the measured values.

A1 2 (5c) If suitable meteorological data are available for the respective site, the statistical calculation method may also be applied for the determination of the dispersion parameters.

A1 2 (6) Any releases of radioactive materials via the exhaust air path are taken into account in the calculation of the possible radiological consequences of events on level of defence 3.

A1 2 (7) Radiation exposure is determined by considering the exposure paths of external irradiation, inhalation and ingestion. Any restrictions of utilisation following the onset of an event on level of defence 3 are taken into account in the calculation of radiation exposure.
N o t e: Assumptions on consumption behaviour and restrictions of utilisation are specified in the Radiological Accident Calculation Bases (see in subsection A1 2 (1)).

A1 2 (8) Furthermore, the actual conditions in the surroundings of the site are taken into account in the calculation.

A1 2 (9) Other than stipulated in the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1), subsection 3.1 (8), it may be assumed when calculating the radiological consequences of events on level of defence 3 that the first actuation of the reactor protection system or the first actuation of reactor scram will become effective if not impaired itself by the corresponding event.

A1 2 (10) Other than stipulated in the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria " (Module 1), subsection 2.1 (5), the calculation of the radiological consequences of events on level of defence 3 may take the operational installations that contribute to damage mitigation into account if these installations have been manufactured and are operated in line with applicable codes and guides, if they possess suitable quality features with regard to their design and proven service records and if their operability is not impaired by the consequences of the respective events.

A1 2 (11) A single-failure beyond the application of the single failure concept according to the "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components" (Module 10), Section 1.1 for aggravating the respective boundary conditions in the analysis to verify the limitation of radiation exposure of the population is not postulated.
N o t e: For verifying the limitation of radiation exposure of the population on level of defence 3 according to the requirements of the Radiation Protection Ordinance, further boundary conditions are defined by the "Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation" (Module 6), Section 3.2.4.

J

MODULE 10
"Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components"

Contents

0 Objectives and scope

This guidance text contains safety-related criteria for the design and safe operation of safety-relevant structures, systems and components.

Further, specific criteria for design and operation of installations in nuclear power plants are to be found separately in the “Safety Criteria for Nuclear Power Plants:”
- “Criteria for the Design and Operation of the Reactor Core” (Module 2),
- "Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System" (Module 4),
- "Criteria for Instrumentation and Control and Accident Instrumentation" (Module 5),
- "Criteria for Accident Management" (Module 7),
- "Criteria for Radiation Protection" (Module 9),
- "Criteria for the Handling and Storage of the Fuel Elements" (Module 11),
- "Criteria for Electric Power Supply" (Module 12).

For installations not included in them, generally accepted engineering standards, e.g. the conventional rules and regulations, are applicable regarding the case of application. If generally accepted engineering standards are applied they have been reviewed for compliance with the state of the art on a case-by-case basis.

1 General criteria

1.1 Criteria for the control of single failures

N o t e: The single failure assumption is a deterministic concept for the design of safety-relevant installations in nuclear power plants. Regarding the design of safety-relevant installations in nuclear power plants, the postulation of a single failure serves to ensure sufficient redundancy and segregation. If a safety-relevant installation is designed according to the single failure concept it can be assumed with sufficient certainty that its operability is not dependent on the coincidental failure of any particular component of the installation.

The following criteria represent a concrete expression of the principles on the single-failure concept formulated in the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1).

1.1 (1) The degree of redundancy of installations required for ensuring a safety function depends on its safety relevance within the defence-in-depth concept.

1.1 (2) A single failure does not lead to safety-relevant failures of safety-relevant installations for ensuring a safety function in other redundants.

1.1.1 General redundancy criteria for operating phases A and B

N o t e: For the definitions of the operating phases, see “Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors” (Module 3)

1.1.1.1 Redundancy criteria for installations of level of defence 1

For installations of level of defence 1, there is no requirement for redundant design (degree of redundancy n+0).

1.1.1.2 Redundancy criteria for installations of level of defence 2

1.1.1.2 (1) For installations for the control of events on level of defence 2, neither a single failure nor unavailability of a redundant due to maintenance measures (maintenance case) are postulated (degree of redundancy n+0).

However, for the instrumentation and control (I&C) functions of Category B, degree of redundancy n+1 applies (see “Safety Criteria for Nuclear Power Plants: Criteria for Instrumentation and Control and Accident Instrumentation“ [Module 5], Section 3.3).

1.1.1.2 (2) Maintenance work on installations performing I&C functions of Category B (see “Safety Criteria for Nuclear Power Plants: Criteria for Instrumentation and Control and Accident Instrumentation“ [Module 5]) is only performed under consideration of specified permissible maintenance times.

1.1.1.3 Redundancy criteria for installations of level of defence 3

1.1.1.3 (1) For the safety installations required for the control of events on level of defence 3, single failure principally coupled with the maintenance case is postulated in case of challenge (degree of redundancy n+2).

For the maintenance cases, all maintenance measures that can be performed during the respectively relevant operating phases are considered.

If for a safety installation, a redundancy degree of only n+1 is realised (e.g. for primary circuit or containment isolation valves), maintenance measures are only performed if during the maintenance-induced unavailability of such an installation, its safety-related function is reliably ensured otherwise by substitute measures (e.g. closure of the 2nd isolation valve as a precaution).

1.1.1.3 (2) Maintenance work on installations of level of defence 3 is only performed under consideration of the criteria according to Section 1.2 (degree of redundancy temporarily reduced to n+1).

1.1.1.4 Redundancy criteria for installations of level of defence 4a

1.1.1.4 (1) For installations required for the control of events on level of defence 4a, neither single failure nor maintenance is postulated in case of challenge (degree of redundancy n+0).

1.1.1.4 (2) As far as the function of installations is required within 30 minutes for the control of impacts from man-made hazards aircraft crash and explosion blast wave, single failure is postulated for active components of these installations (degree of redundancy n+1).

1.1.1.5 Redundancy criteria for installations of level of defence 4b and 4c

For installations of levels of defence 4b and 4c, neither single failure nor maintenance case is postulated (degree of redundancy n+0).

1.1.2 General redundancy criteria for safety installations for the operating phases C to F

1.1.2 (1) For the periods of scheduled maintenance work during operating phases C to F on installations of level of defence 3 required for these operating phases, a single failure but no additional maintenance case is postulated (degree of redundancy n+1).

1.1.2 (2) A degree of redundancy n+0 is permissible in the operating phases E and F if in case of failure of the safety installation, the time until non-fulfilment of the acceptance criteria is more than 10 hours and the active safety-relevant installations failed or being under maintenance are available within this time.

1.1.3 Specific criteria

1.1.3.1 Single failure assumptions for active and passive installations

1.1.3.1 (1) For active installations, single failures are always postulated and for passive installations generally postulated. Exceptions are justified.

1.1.3.1 (2) For passive installations, single failure is not postulated if it has been demonstrated that they fulfil at least the criteria regarding design, construction, material selection, manufacturing, testability and operating conditions for the external systems according to the “Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System“ (Module 4).

1.1.3.1 (3) Non-return valves belong to the passive installations if, when challenged, they do not have to change their initial position for fulfilment of the safety function.

1.1.3.2 Determination of the most unfavourable single failure

Regarding the fulfilment of the respective acceptance criterion, the most unfavourable single failure is justified.

1.1.3.3 Combination of single failure and maintenance case

If simultaneous maintenance is postulated according to the safety-related redundancy degree criteria, the all in all most unfavourable combination of a single failure with the maintenance case is considered.

1.1.3.4 Single failures due to operating error

A potential operating error leading to a malfunction of installations is considered equal to a single failure.

1.1.3.5 Single failures in pilot-operated valves

For self-medium-operated safety valves, relief valves and isolation valves of the reactor coolant system and the main steam system, required for accident control, single failure in the pilot control is postulated.

1.1.3.6 Single failures in several installations required for controlling the case of challenge

If several installations have to fulfil their tasks simultaneously or subsequently for controlling a postulated case of challenge, occurrence of a single failure is postulated for the total of the systems but not in several of the installations required at the same time.

1.2 Maintenance measures on safety-relevant installations

Detailed plant operating procedures exist for maintenance.

1.2.1 Maintenance measures for achieving the specified normal condition of a safety-relevant installation (repair)

Maintenance measures for achieving the specified normal condition of a safety-relevant installation for which case of challenge in combination with maintenance is postulated according to the criteria of Section 1.1.1 are permissible within the times specified in the plant operating procedures.

1.2.1.1 Criteria in case of deficiencies identified in safety-relevant installations

1.2.1.1 (1) In case of deficiencies identified in safety-relevant installations that lead to the unavailability of the installation when challenged, measures for identifying the cause of the deficiency and for removing the deficiency are initiated immediately.

1.2.1.1 (2) If a deficiency identified leads to the unavailability of a safety-relevant installation, the repair times to be determined according to Section 1.2.1.2 shall be applied. In cases where the plant operating procedures do not include explicit specifications on permissible repair times for safety installations, the plant is immediately brought into an operating condition in which the availability of this installation is not required or to a limited extent. The plant operating procedures include instructions on the determination of an appropriate operating condition for such cases.

1.2.1.2 Specification of permissible repair times

The permissible unavailability times of installations for the control of events on levels of defence 2 to 4a are determined and specified in the plant operating procedures. In particular, these specifications include the following information:

– Permissible duration of unavailability of one or more of these installations and / or their minimum availability for each operating phase.
– Clear description of the measures to be initiated when reaching the limit of the permissible unavailability times (e.g. power restriction or plant condition to be reached, measures for reducing the occurrence probability of events).

1.2.1.3 Measures in case of predictable excess of permissible repair times

If in case of an identified deficiency in a safety-relevant installation, for which the permissible repair times are specified, it can be foreseen that repair cannot be performed within the permissible time, the measures provided according to Section 1.2.1.2 are initiated immediately.

1.2.1.4 Servicing of safety installations

If servicing is required for ensuring the functional operability of safety installations, these can always be performed without any special restrictions if
– servicing measures only lead to unavailability times of the safety installation of less than 8 hours, and
– the safety installation can be rapidly restored to the operating condition in case of challenge, also under the conditions of the incident occurred, and
– the work remains restricted to one redundant.

1.2.2 Criteria for preventive maintenance in the operating phases A and B

1.2.2.1 Permissibility of preventive maintenance during operation (PMO) in dependence of the required degree of redundancy

1.2.2.1 (1) The duration and the boundary conditions under which PMO on installations for the control of events on levels of defence 2 to 4a in the operating phases A and B is permissible are specified in the plant operating procedures under consideration of the safety-related requirements.

1.2.2.1 (2) Regarding the specifications, the following criteria are fulfilled:
– If PMO is performed on installations of level of defence 3, the redundancy degree of the installations is higher than or equal to n+2. In case of n+3 and higher redundant safety installations, there are no criteria for PMO in a single redundant beyond the criteria according to Section 1.2.2.2.
– For n+2 installations of level of defence 3, the time of unavailability due to PMO is restricted under consideration of the reliability requirements for the respective safety installation. For n+2 installations, the duration of unavailability does not exceed 7 days per redundant and year. For longer periods, justifications are available in form of plant-specific individual demonstrations.
– Installations of level of defence 2 with a degree of redundancy of n+1 are only subjected to PMO if an assessment of sufficient reliability of the installations under consideration of the relevant cases of challenge was performed.
– Installations of level of defence 4a are only subjected to PMO if an assessment of sufficient reliability of the installations under consideration of the relevant cases of challenge was performed.

1.2.2.2 Special criteria

PMO measures beyond the criteria of Section 1.2.2.1 are only permissible if the following boundary conditions are fulfilled:
– The PMO measure does not lead to a noteworthy increase of occurrence probability for events on levels of defence 2 and 3.
– PMO measures are not performed in several redundants at the same time but are limited to one redundant.
– The PMO measure does not lead to failures of safety-relevant installations not being affected.

– The PMO measure does not increase the possibilities of common-cause failures of safety-relevant installations.
– The fulfilment of the criteria for maintenance measures in case of PMO is also ensured under the conditions of operating phases A and B (e.g. unrestricted feasibility of functional tests after maintenance).
– The integrity of the two barriers reactor coolant pressure boundary and containment and the reliability of their safety-related functions will not be impaired by PMO measures in an undue manner.

1.3 Prevention of multiple failures

1.3 (1) Appropriate measures and installations against common-cause failures of several safety installations redundant to each other are realised, applying the design principles according to the "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" (Module 1), subsection 3.1 (3).

1.3 (2) Safety installations for which potentials for common-cause failures were identified are designed according to the principle of diversity as far as feasible and technically reasonable.

1.3 (3) Redundant installations are physically or constructionally separated such that potentially redundancy-wide internal or external events remain limited to one redundant of the installations required for the control of postulated accidents according to the "Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors" (Module 3). Regarding man-made hazard conditions, it is ensured for installations of level of defence 4a that in case of an event one redundant remains available. Here, any consequential impacts are also taken into consideration.

1.3 (4) As far as common components for various redundants, e.g. testing devices, are inevitable, it is ensured that potential failure mechanisms at these components and the connecting parts do not lead to impacts affecting more than one redundancy.

1.3 (5) Maintenance measures are organised and designed such that operating errors of the personnel remain limited to one redundancy. Further, a redundancy-wide erroneous use of auxiliary and operating materials (e.g. lubricants, sealings) is prevented by suitable quality assurance measurements.

1.3 (6) The in-service inspections of redundant installations are organised by appropriate measures, e.g. scheduling, such that redundancy-wide failures are prevented or identified and removed as early as possible.

1.3 (7) Deficiencies and damages in safety-relevant installations are analysed with regard to their cause. Here, it is clarified, in particular, whether the damage mechanism identified is of systematic nature. If there is suspicion of a systematic failure, it is clarified immediately and corrective measures are taken, if necessary. The necessary safety-related measures when determining redundancy-wide failures are included in the plant operating procedures.

1.4 Ensuring the functional readiness of safety-relevant installations

1.4 (1) The function of safety-relevant installations is checked under conditions that correspond to the case of challenge as far as possible to the required extent.

1.4 (2) The performance of functional tests does not lead to a noteworthy increase of occurrence probability for events on levels of defence 2 and 3.

1.4 (3) If possible, the entire functional sequence of the respective installation as happens in case of challenge is subjected to a functional test, e.g. also switching of emergency power supply to the consumers. If subtests are necessary for process-related reasons, valid overlapping of the various subtests is ensured.

1.4 (4) The functional readiness of the installations is also maintained during the functional test as far as possible. Where applicable, downtimes due to tests performed are considered in the reliability analysis.

1.4 (5) It is ensured that test-induced deviations from the readiness state of a safety installation can be removed in due time if a case of challenge occurs.

1.4 (6) The functional readiness of a safety-relevant installation is ensured. Scheduled or fault-induced unavailabilities (e.g. deviation from readiness state, unavailability due to maintenance) of individual components leading to an unavailability are identifiable for the operating personnel. Erroneous positioning of valves is prevented as far as possible by reliable technical installations and / or organisational measures.

1.4 (7) Deviations from parameter values specified in the plant operating procedures for ensuring safe plant operation are indicated to the operating personnel by optic and acoustic signals at the control room.

1.4 (8) It is ensured that for a case of challenge all information necessary for the assessment of the functional readiness and effectiveness of installations required in case of challenge are available to the operating personnel at the control room or the emergency control room or can be easily and rapidly determined by the information available at the control room or the emergency control room.

1.4 (9) The functional readiness and the function of safety-relevant installations according to the requirements are ensured after completed maintenance by qualified functional tests.

2 Criteria for the control of internal events

2.1 General criteria

2.1 (1) The internal events according to "Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors" (Module 3) that may occur due to the plant-specific conditions are considered.

2.1 (2) For each event, its safety-related impacts on the plant under consideration of the consequential impacts to be expected are determined. In particular, the effects listed in the following are considered:
- Plant-internal flooding,
- plant-internal fires,
- increased radiation level,
- chemical reactions,
- electrical, I&C or process related malfunctions/failures,
- pressure build-up, pressure differences,
- temperature and humidity increase,
- fragments (debris) flying around and falling, as well as
- jet and reaction forces.

2.1 (3) Installations for the protection against impacts are preferably installed near to the potential source of an internal event.

2.2 Event-specific criteria

2.2.1 Plant-internal fire

Note: For the facts and circumstance dealt with in the following, relevant requirements of the conventional rules and regulations are also applicable.

2.2.1 (1) Measures and installations for the protection against fires and their consequences are both provided inside and outside of buildings.

2.2.1 (2) Fire protection measures are planned and implemented such that defence in depth is realised:

- Measures and installations are provided that prevent the outbreak of fires.
- Fires breaking out in spite of it are quickly detected and fought.
- Spread of a fire not extinguished or not going out is limited.

2.2.1 (3) The fire resistance of building groups, individual buildings and structures within buildings is ensured by structural fire protection measures. Spread of fire over several buildings is prevented and remains limited within a controllable area in the building.

2.2.1 (4) A plant-specific fire protection concept is developed and documented. The documentation is kept up to date. In order to verify the adequacy of the fire protection concept and the fire protection measures defined in it, a fire hazard analysis is performed.

2.2.1 (5) Ignition of flammable materials is generally postulated.

2.2.1 (6) Fire loads and potential ignition sources are minimised.

2.2.1 (7) An alarm plan is developed for measures to be taken in the event of a fire.

2.2.1 (8) The use of combustible materials as construction elements or as operating supplies is generally avoided. In areas where the use of such materials cannot be avoided, appropriate measures are taken which prevent the outbreak of fires and limit their spread and minimise the generation and spread of smoke. All construction materials are at least flame retardant.

2.2.1 (9) As far as larger amounts of unprotected combustible materials are located in rooms with safety-relevant installations and equipment or in rooms from where a fire may spread into adjacent rooms with safety-relevant installation, quick acting fire extinguishing systems are provided for them. Automatic fire extinguishing systems are protected against inadvertent actuation or the rooms in which such extinguishing systems are installed are protected against the impacts of an inadvertent actuation. When introducing combustible materials in connection with maintenance work, special measures and installations are provided.

2.2.1 (10) The layout of the redundants of the safety system is generally such that in case of fire a loss of more than one redundant due to fire-induced heat, fumes or fire extinguishing agents does not have to be postulated.

2.2.1 (11) If sufficient physical separation is not feasible, the redundants are at least sealed off or encapsulated with a fire resistance class that corresponds to the fire load.

2.2.1 (12) As a matter of principle, lines and cables of safety-relevant I&C installations are laid separately from heated pipes or such that carry combustible media. Power cables are sufficiently separated from signal and control cables. In case of unavoidable crossings, special measures and installations are provided. Measures and installations are provided against impairment of safety-relevant cables by fire as well as against spread of fire along safety-relevant cables.

2.2.1 (13) Plant areas with safety installations and controlled areas as well as plant areas from which a fire may spread into plant areas with safety installations or controlled areas are equipped with an adequate instrumentation for an early detection of fires. The equipment for the early detection of fires are designed with a sufficient degree of reliability.

2.2.1 (14) The removal of fire-related heat and gases does not endanger the function of escape routes and redundants of safety-relevant installations not immediately affected by the fire. If the compartment ventilation systems are used for the removal of smoke, these are designed in accordance with the thermal stresses to be anticipated. If necessary, special smoke and heat removal equipment shall be provided. The separation of the individual fire compartments and fires cells is ensured by ventilation ducts or fire protection shutters in the ventilation ducts in the area of the walls, ceilings and floors.

2.2.1 (15) The restrictions existing in the controlled area are considered in the selection and installation of active and passive fire protection features.

2.2.1 (16) The fire protection installations are regularly subjected to in-service tests with respect to their operability. The testing intervals are determined in accordance with the safety significance of the installation to be protected.

2.2.1 (17) The fire detection and alarm systems and the fire extinguishing systems in the containment are reliable and effective to a degree that fires can also be localised reliably and fast and fought effectively without removing smoke from the containment.

2.2.1 (18) Due to the measures and installations according to subsection 2.2.2 (2), a single failure remains without safety-related consequences.

2.2.1 (19) From among the operating personnel, a fire brigade is established according to the law of the *Länder* (also referred to as plant fire brigade). In addition, the competent local fire brigade was also familiarised with the compartments of the plant and with the special conditions prevailing at a nuclear power plant. The corresponding instructions are repeated at regular intervals. Fire drills are held at adequate intervals.

2.2.1 (20) It is ensured that all measures required for ensuring safe operation and control of events on levels of defence 3 and 4a can also be performed in the case of fire fighting.

2.2.2 Plant-internal flooding

2.2.2 (1) Measures and installations are provided for the prevention of plant-internal flooding, including

- high-quality design of the medium containing components,
- precise specifications for maintenance measures on medium containing components, in particular those with high flooding potential,
- high reliability of automatic extinguishing systems.

2.2.2 (2) Potential initiating events for flooding within the plant are identified (e.g. leaks, actuation of a fire extinguishing system, human errors, drop or hitting of loads, startup of systems with isolation devices inadvertently not installed). Enveloping events are defined wherever possible.

2.2.2 (3) If maintenance measures are performed on installations for the prevention of flooding events, it is ensured that their function, if required, also remains ensured during the maintenance measure or is fully compensated by other measures by way of precaution. The areas particularly endangered in connection with maintenance measures are, among others, the sump suction lines and their isolation valves, lines with a high fill-up potential and their isolation devices, installations for the prevention of redundancy-wide flooding in the annulus of PWR plants as well as maintenance work in the bottom area of reactor pressure vessels of BWR plants.

2.2.2 (4) Safety-relevant impacts of an accumulation of water at structures located at an elevated level (e.g. cable racks with insufficient drainage) are covered in flooding analyses.

2.2.2 (5) For all flooding events postulated, the anticipated time history of the water level in the rooms affected directly and in the potentially affected adjacent rooms is considered.

2.2.2 (6) The possibility of clogging of drainage structures and of a displacement of objects and small particles is taken into account.

2.2.2 (7) For the determination of the flooding level and of the mechanical impacts on components or barriers, potential formation of waves is considered.

2.2.2 (8) A possible pressure increase due to the contact of water with hot components is considered.

2.2.2 (9) For postulated flooding events, measures and installations for the control or prevention of undue safety-related impacts are provided. Here, the following measures and installations are considered, in particular, according to a graded proceeding:
- leak monitoring systems,
- measures for the detection and isolation of leak locations,
- installation of safety-relevant components at an elevated level,
- structural provisions (e.g. drain pans, shieldings) around safety-relevant components,
- guard pipe design,
- barriers or equivalent installations for preventing spread of water, in particular into other redundants,
- active and / or passive installations for drainage,
- organisational measures for a flooding event (e.g. provision of measures and installations for drainage).

2.2.2 (10) In addition to the direct impact of a flooding, indirect effects, such as increased humidity, are also considered.

2.2.3 Component failure with potential impacts on safety-relevant installations

2.2.3 (1) The function of safety-relevant installations is reliably protected against the following impact of a postulated component failure:
- Direct mechanical impacts (reaction forces, whipping pipes),
- jet forces,
- flooding,
- increased humidity,
- physical or chemical impacts,
- pressure differences (static and dynamic),
- increased room temperature, and
- increased radiation level.

For the leak and break assumptions, the specifications in the “Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors" (Module 3), Annex 2 apply.

2.2.3 (2) For these impacts, the stability of walls, ceilings and internals is also analysed.

2.2.3 (3) Damages at safety-relevant components due to pipe whip are preferably prevented by structural provisions for the pipes.

2.2.3 (4) All potentially safety-relevant sources for high-energy fragments are identified and the parameters (in particular geometry, mass and trajectory) of the fragments to be expected in case of a failure are analysed or assessed conservatively.

As potential sources for high-energy fragments, the following is considered in particular:
- Failure of high-energy vessels and other components,

Note: For the leak and break assumptions, see “Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors" (Module 3), Annex 2.

- failure of movable valve components,
- ejection of a control element or rod, and
- failure of rotating component parts (e.g. flywheel failure of the main coolant pumps,, turbine blades, turbine shaft).

2.2.3 (5) As far as high-energy fragments and resulting endangerment of safety-relevant installations cannot be precluded, precautions are provided for the protection of these installations.

2.2.3 (6) Here, the following measures and installations are taken into consideration:
- appropriate orientation of the components in the compartment identified as potential source of fragments,

– appropriate spatial layout of the safety-relevant installation identified as potential targets of fragments,
– selection of building arrangement such that safety-relevant installation are not located within the probable flight direction of potential fragments of the turboset. This also applies to multi-unit plants,
– structural provisions for deflection or retention of debris,
– pipe whip restraints,
– guard pipe design for high-energy pipes.

N o t e: Specific relevant criteria are to be found in "Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System" (Module 4), Section 6.

2.2.3 (7) If safety-relevant impacts are to be expected in case of failure of rotating components,
– reliable installations are provided for limiting the speed, and
– for identification of damages initiated by unbalances (vibration monitoring).

2.2.3 (8) Precautions are taken to ensure that the flywheels of the main coolant pumps (PWR) are not destroyed during a loss-of-coolant accident due to excessive speed.

2.2.3 (9) For barriers for protection against high-energy-fragments, both the local (e.g. penetration, spalling) and the global load-bearing and deformation behaviour of the barrier during impact of the high-energy fragments on the barrier are considered.

2.2.3 (10) As far as a double-ended rupture of a high-energy pipe is to be postulated regarding the control of jet and reaction forces according to the "Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors" (Module 3), Annex 2, precautions are taken against safety-relevant damages due to such a rupture.

In particular, the following aspects are considered:
– Pipe whip direction,
– safety-relevant installations affected,
– kinetic energy,
– amount of energy absorbed by a component affected,
– effectiveness of pipe whip restraints, and
– potential consequential impacts in case of impact on other components.

2.2.4 Drop and impact of loads with potential endangerment of safety-relevant installations

2.2.4 (1) Loads that may lead to the failure of safety-relevant installations or the release of radioactive material when dropping are identified. These also include roll-over and impact of swinging objects, in particular also of transport and storage casks.

The stability of the transport and storage casks is given for all set-down positions, generally also in case of external events postulated at levels of defence 3 and 4a, for aircraft crash only with regard to its consequential impacts.

Exceptions are limited to short-term, unavoidable set-down of the cask during the transport and handling process. The duration of set-down on these positions is limited to the time required.

N o t e: See also "Safety Criteria for Nuclear Power Plants: Criteria for the Handling and Storage of the Fuel Elements (Module 11), subsection 7.3 (2) and 7.4 (1).

2.2.4 (2) As cause for drop of loads, faulty operation or maintenance on lifting equipment as well as on or with its hoisting gears, load-bearing and load attachment devices are also considered.

2.2.4 (3) It is ensured that drop of load with uncontrollable consequences is not to be postulated (see also Section 5.2.9).

2.2.5 Electromagnetic impacts

2.2.5.1 General criteria

2.2.5.1 (1) Safety-relevant installations work reliably in their electromagnetic environment.

2.2.5.1 (2) An analysis of electromagnetic compatibility (EMC analysis) is performed to the required extent. It comprises the electromagnetic interference radiation, the disturbance resistance of the components and the necessary tests.

2.2.5.1 (3) During the lifetime of the plant, both the occurrence of new and the change of existing sources of interference are monitored. The protection of safety-relevant installations against electromagnetic influences is adapted to changed environmental conditions, if necessary.

2.2.5.2 Prevention of impermissible sources of interference

2.2.5.2 (1) Potential electromagnetic interferences inside the plant are identified and assessed. Enveloping sources of interference are considered to the extent possible. The resulting environmental conditions at the location of operation are determined.

2.2.5.2 (2) The generation of electromagnetic interference is limited such that proper functioning of the safety-relevant electrical installations is given.

2.2.5.2 (3) For limitation of electromagnetic influences from plant-internal sources, measures and installations are provided for I&C protection according to their safety significance (e.g. shielding, decoupling, earthing, spatial separation).

2.2.5.2 (4) Temporarily existing potential sources of interference, as for example measuring and testing devices, welding equipment or mobile phones, are considered.

2.2.5.2 (5) Interference-induced electromagnetic interactions (short circuit, electric arc) are considered.

2.2.5.3 Protection of installations against impermissible electromagnetic impacts

For safety-relevant installations that may be impaired by electromagnetic impacts, it is demonstrated by tests that their electromagnetic compatibility is given in their operation environment.

2.2.6 Collision of vehicles at the plant site with safety-relevant structures, systems or components

Safety-relevant structural plant components, systems or components at the plant site are designed or protected by installations such that they are not impaired in their safety function by collisions with vehicles at the plant site.

2.2.7 Mutual influence between multi-unit plants and neighbouring plants

2.2.7 (1) Events on levels of defence 2 to 4a do not lead to an undue impairment of the safety of the neighbouring unit.

2.2.7 (2) Electrical and process-related connections between units that have the same safety function in the units are permissible if the reliability of this safety function is not impaired.

2.2.7 (3) For events with radiological consequences, it is ensured that the neighbouring unit can be kept in a safe condition.

2.2.8 Explosion protection

N o t e: For the facts and circumstances dealt with in the following, relevant requirements of the conventional rules and regulations are also applicable.

2.2.8.1 General criteria

2.2.8.1 (1) Measures and installations of explosion protection secure the function of safety-relevant plant components.

2.2.8.1 (2) Measures and installations are provided for the prevention of chemical explosions, explosions of steam-gas mixtures, BLEVEs (boiling liquid expanding vapour explosions) and physical explosions inside and outside of buildings as far as the initiating materials are stored or handled in the area of the plant in relevant amounts or if they can be produced there.

2.2.8.1 (3) The explosion protection measures are planned and designed such that defence in depth is realised. For this purpose, measures and installations are provided that

- prevent or limit the generation of an explosive atmosphere,
- prevent ignition of an explosive atmosphere generated despite the provisions, and
- limit the consequences of an explosion such that undue safety-related impacts do not occur.

2.2.8.1 (4) If formation of explosive gas mixtures cannot be excluded, special measures are taken and / or installations provided:

- Limitation of the amounts of explosive gas,
- elimination of all potential ignition sources, encapsulation of ignition sources that cannot be avoided,
- adequate ventilation, and
- use of installations and tools, in particular electrical devices, qualified for the use in explosive atmospheres.

2.2.8.1 (5) The consequences of postulated explosions are minimised by measures and installations, such as

- pressure relief systems,
- observance of safety distances to safety-relevant installation, and
- protective measures such as partition walls.

2.2.8.1 (6) All postulated explosions are assessed regarding their impacts on safety-relevant installations.

2.2.8.1 (7) The possibility of explosive processes due to the effects of fire is minimised either by physical isolation of potential fire sources from explosive substances or by active measures.

2.2.8.1 (8) If it is necessary to keep explosive materials available on the plant site, the following principles are applied:

- The amount of explosive materials is minimised.
- Proper storage is ensured.
- Sufficient distance to potential ignition sources is kept.
- Fire and gas alarm systems and, where appropriate, automatic extinguishing systems are provided at the storage location.

2.2.8.1 (9) Fire is considered as consequential event of explosions.

2.2.8.1 (10) Pressure waves not due to an explosion are also taken into consideration.
Note: These are, for example, pressure waves resulting from electric arcs in electric medium and high-voltage switchgears.

2.2.8.2 Prevention of undue effects of radiolysis gas reactions in systems and components
Note: The following criteria are mainly applicable to plants with boiling water reactors.

2.2.8.2 (1) Measures and installations are provided for the prevention of radiolysis gas accumulations and, if necessary, for mitigating the consequences of radiolysis gas reactions.

2.2.8.2 (2) The measures and installations consider all system areas that may be loaded with steam of reactor coolant.

2.2.8.2 (3) Extent and quality of the precautions to be taken are oriented towards the maximum effects of the postulated radiolysis gas reactions. It is ensured that impacts not controlled by installations of level of defence 3 do not occur.

2.2.8.2 (4) For the determination of the system areas affected, all operating conditions, operating processes and disturbed conditions are considered. The accumulation of radiolysis gas by condensation of steam containing radiolysis gas on cold media is taken into consideration.

2.2.8.2 (5) If radiolysis gas accumulations cannot be excluded for process-related reasons, enveloping radiolysis gas accumulations and reactions are postulated for the determination of precautions to be taken,.

In case of permanent turbulent flows in a system area, accumulation of radiolysis gas can be excluded there.

The reaction pressure and the impacts on the plant, the system and neighbouring components by fragments and blast waves as well as by loss of coolant, jet forces, increased radiation level, reaction forces, temperature and humidity are determined.

2.2.8.2 (6) The effectiveness of the measures and installations provided is continuously monitored or demonstrated by in-service inspections.

2.2.8.2 (7) Passive provisions, such as forced flow, are preferred to active ones.

2.2.8.3 Prevention of explosive hydrogen mixtures in the containment

To prevent any hydrogen explosion or hydrogen fire inside the containment during specified normal operation (levels of defence 1 and 2) as well as for events on level of defence 2, the ignition limit of hydrogen (4% hydrogen in the air) is not exceeded at any time, neither integrally nor locally. All sources of hydrogen formation are considered.

N o t e: The specifications to be considered when determining hydrogen formation and release are included in Annex 1 of “Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation" (Module 6).

For accident management measures regarding the prevention of explosive hydrogen mixtures see “Safety Criteria for Nuclear Power Plants: Criteria for Accident Management" (Module 7), subsection 4.2 (4).

2.2.8.3.1 Monitoring of the hydrogen concentration in containment compartments after loss-of-coolant accidents

2.2.8.3.1 (1) A measuring system is available which ensures reliable determination of the hydrogen distribution within the primarily loaded areas of the containment even under the conditions to be expected after a loss-of-coolant accident.

2.2.8.3.1 (2) On the basis of appropriate calculation methods, measuring points are defined that enable reliable monitoring of the hydrogen concentrations.

2.2.8.3.1 (3) At the measuring points for determination of the hydrogen concentration, the temperature in the containment is also measured.

2.2.8.3.2 Prevention of explosive hydrogen concentrations after loss-of-coolant accidents

2.2.8.3.2 (1) The following principles apply to measures and installations for the prevention of explosive hydrogen concentrations in the containment atmosphere after a loss-of-coolant accident:

a) If the calculations reveal that the hydrogen concentration may reach values above the ignition limit in certain areas of the containment, measures are provided which ensure sufficient forced flow mixing of the containment atmosphere.
b) If the calculation of the integral hydrogen concentration reveals that reaching the ignition limit cannot be excluded in the long term, the following shall apply:

(i) It is shown that the possibility to connect recombiners to the containment in an adequate manner is provided or that a recombiner system is installed that fulfils the criteria of level of defence 3.
(ii) It shall be ensured that during an incident recombiners are made of use of in time and in a reliable manner.
(iii) The recombiner depletion rate shall be dimensioned such that the integral hydrogen concentration in case of maximum initial loading by hydrogen, in particular originating from Zr-water reaction, always remains below the ignition limit.
(iv) The design of the recombiners ensures their reliable availability and function even under the conditions prevailing within the containment at the moment of necessary activation. It is demonstrated that the fission product load of the recombiners determined under conservative boundary conditions will not unduly impair their function under radiological aspects and aspects important to safety by airborne halogens and volatile solids and the resulting heat tone in the recombiners.
(v) With regard to the possibility of significant activity quantities being displaced from the containment vessel into the recombiner train after an accident, the recombiners outside the containment are installed as near as possible to the containment with respect to accessibility. This location and other rooms outside of the containment, which are penetrated by the inlet and outlet pipes of the recombiner system, are ventilated through aerosol and iodine filters in order to prevent undue radioactive releases through possible leaks. The pipes are shielded accordingly.

2.2.8.3.2 (2) It is possible to use active measures in time before a postulated hydrogen concentration of 4% volume content is reached. Actuation may be effected manually.

2.2.8.3.2 (3) Flushing of the containment (injection and discharge from the containment) is not planned for the reduction of the integral hydrogen concentration.

2.2.8.3.2 (4) A single failure is not postulated for non-stationary recombiner systems as far as repair or substitute measures will be possible in time.

3 Criteria for the control of external events

3.1 General criteria

3.1 (1) The natural and human-induced external events are determined site-specifically and classified with regard to their classification according to the levels of defence according to the “Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors“ (Module 3).

3.1 (2) On the basis of a deterministic analysis under consideration of analyses on the frequency of the events and its sequence, measures are taken and installations provided so that impermissible impacts on the plant are not to be postulated.

3.1 (3) Regarding the design of the measures and installations, the impacts on the plant under consideration of the time-dependent sequence of the event and all consequential impacts to be expected are determined and taken into account for each event considered.

3.1 (4) A permanently effective protection is generally realised by the measures and installations.

3.1 (5) For events with sufficiently slow time-dependent development, additional temporary installations kept available may be used.

3.1 (6) Continuously and short-term variable parameters of external events and derived predictions on the further development of safety-relevant parameters are observed and considered anticipatory..

This applies, in particular, to the receiving water level and temperature for the safety-relevant cooling water supply and to the outside air temperature.

Limits and preceding intervention levels are defined where measures are taken in due time if these are exceeded.

3.1 (7) After an event leading to an excess of the preceding specified value (intervention value), it is checked whether there were retroactions on the safe operation of the plant or on safety-relevant installations.

3.1 (8) During long-lasting impacts, safety inspections are performed at appropriate intervals.

3.1 (9) Specifications with regard to combinations of various external events and of other events to be considered are included in the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1), subsection 4.1 (5), as well as in the “Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation" (Module 6), subsection 3.2.4 (7), 3.2.4 (8) and 3.2.5 (4).

3.1 (10) External events and resulting loads are principally combined with the specified static and dynamic loads during operation for the respective structures and systems. For short-term and low frequent operational loads and related plant conditions, it is permissible to deviate from it.

3.1 (11) In case of overlapping events, their time-dependent development is taken into consideration.

3.1 (12) The external events considered according to subsection 3.2.1 (1) also comprise those impacts that are covered by another external event at the same level of defence.

After modification of the measures and installations against an enveloping event, the enveloping character of the provisions is verified again.

3.1 (13) The protection concept provided against external events is documented in a revisable manner.

The documentation includes at least a listing of the events considered including their primary effects and consequential impacts as well as verification of appropriateness and sufficient reliability of the provisions taken.

3.2 Event-specific criteria

3.2.1 Man-made hazards

3.2.1.1 Aircraft crash

3.2.1.1 (1) The plant components to be protected against accidental aircraft crash are determined.

3.2.1.1 (2) The description of the safety-related functions of these plant components as well as the way how the stability of the structures and of the entire plant will be assured when stresses occur is documented.

3.2.1.1 (3) The design is based on the following load assumptions:
1. Impact-load time diagram

Impact time [ms]	Impact load [MN]
0	0
10	55
30	55
40	110
50	110
70	0

2. Impact area: 7 m2 circular
3. Impact angle: normal to the tangential plane at the point of impact.

3.2.1.1 (4) Structures are designed to afford full protection wherever they accommodate safety-related components which may be damaged by concrete missiles and control of the event is no longer ensured in case of failure of these plant components.

3.2.1.1 (5) The effects of missiles, burning kerosene, kerosene explosions and other consequential effects are considered, i.e., in particular,
– burning kerosene at the plant site,
– explosion of the kerosene inventory (in parts or completely) outside of buildings,
– burning or explosion of kerosene (liquid or as steam) which penetrated into buildings though permanently existing openings or those resulting from the crash,
– Intrusion of combustion products and intake air with reduced oxygen content due to combustion processes into ventilation systems under consideration of the impacts on personnel actions, electrical installations and the diesel generator supply air.

N o t e: On this issue, see also Section 2.

The protective effects of structures in front of the one involved in the crash may be taken into consideration. Here, trajectories are considered that may result from the rupture of an aircraft.

For redundant systems, protection against aircraft missiles can also be effected by physical separation.

3.2.1.1 (6) Impacts (e.g. missiles and fires) due to aircraft crashes near the plant are also taken into consideration.

3.2.1.1 (7) The coolant purification ion exchangers of the coolant purification system, associated resin waste tanks and other components and systems which contain comparable high activities in a combustible form on principle are protected by special structural installations and fire fighting measures against damage to prevent a release of considerable amounts of radioactivity resulting from burning kerosene.

3.2.1.1 (8) The shocks induced by the aircraft impact are considered.

3.2.1.2 Plant-external fire

3.2.1.2 (1) If significant fire loads exist in the surrounding area of the plant, it is ensured by measures and installations that plant-external fires do not impair safety-relevant systems in their safety-related function.

3.2.1.2 (2) Here, hot gases and heat radiation are also considered in addition to the impacts by fire and smoke.

3.2.1.2 (3) Ground-level channels and gullies of underground supply installations or buildings are protected against intrusion of combustible liquids.

3.2.1.2 (4) The impacts on ventilation systems, on room temperatures, on the room-sided temperature of the external walls and the intake air of the emergency diesels as well as the potential entry of fumes and smoke into buildings are taken into account.

3.2.1.3 Plant-external explosion

3.2.1.3 (1) The explosion potentials outside the plant are investigated site-specifically.

Here, explosions of steam, gas or liquid clouds, deflagration with partial detonation and physical explosions are considered in addition to chemical explosions.

3.2.1.3 (2) All explosions that cannot be excluded due to the site conditions are analysed regarding their safety-related impacts on the plant.

3.2.1.3 (3) On the basis of these analyses, measures and installations, such as adequate design of structural plant components or safety distances, are provided, if necessary, so that undue safety-related impacts are not to be postulated.

3.2.1.3 (4) In the design against plant-external explosions, the following impacts are considered in particular:
– Direct, reflected and focussed pressure waves,
– time-dependent development of positive and negative pressure,
– debris,
– ground and building vibrations,
– fire and heat.

3.2.1.3 (5) For the structural design and assessment, a conservative pressure distribution is determined on the basis of the analysis according to subsection 3.2.1.3 (2).

3.2.1.3 (6) Local and large-scale explosion effects are taken into consideration.

3.2.1.3 (7) Safety-relevant ventilation systems will not be impaired by explosion impacts in an undue manner.

3.2.1.3 (8) A list of buildings and plant components designed against pressure waves and vibrations caused by them is available.

3.2.1.4 Entry of hazardous materials

N o t e: Hazardous materials are the following:

a) Materials that may lead to a short- or long-term failure of the function of safety-relevant plant components. These are materials that
- are explosive,
- highly inflammable or inflammable,
- displacing or consuming the oxygen contained in the diesel supply air,
- obstructing, or
- corrosive.

b) Materials whose effect will interfere with the adequate assurance of the shift personnel's required capability of action. These are materials that
- are toxic,
- narcotic,
- caustic,
- displacing oxygen,
- consuming oxygen, or
- are explosive, and

c) radioactive materials.

3.2.1.4 (1) Measures are taken and installations are provided against impacts of hazardous materials that may exist at the site. Here, the following aspects are relevant:
– The occurrence of site-related hazardous materials (stationary or on traffic routes),
– their possibilities of getting into the plant,
– their impact mechanisms including the respective time histories (e.g. of the concentration), as well as
– the possibilities of identification and monitoring.

3.2.1.4 (2) To identify the occurrence of hazardous materials and to initiate protective measures, corresponding organisational measures are taken and, to the extent required and possible, installations are provided.

3.2.1.4 (3) Depending on the impacts of the hazardous materials, the following particular measures and installations are taken into consideration apart from the necessary design of the system (e.g. physical separation of the supply openings for redundant plant components):

With regard to the plant,
a) for hazardous materials involving a short-term action
– interruption of the supply of media (e.g. isolation of ventilation systems),
– change in the mode of operation (e.g. from supply air/exhaust air operation to recirculation),
b) for hazardous materials involving a long-term action
– inspection of potentially impaired or for prevention required systems and components including in-service inspections, as well as
– cleaning of these systems and components.

With regard to organisation,
– training of personnel,
– protection of shift personnel including e.g. the availability of respirators, the establishment of areas with an autonomous treatment of media (e.g. air conditioning/regeneration).

In addition,
– detectors for the respective hazardous materials in the supply openings, in the control room, at the power plant site and, where required, in the vicinity of endangered plant components, but primarily in the vicinity of the potential hazardous materials source.
– communications to the place where hazardous materials are handled,
– prevention of long-term contact with corrosive materials,
– protective coatings, and
– safety distances.

3.2.1.4 (4) The accessibility of the control room or emergency control room is also ensured to the required extent during the impact of hazardous materials by the provision of protective equipment.

3.2.2 Other human-induced events

3.2.2.1 Flotsam and ship accidents

3.2.2.1 (1) The supply with coolant required for safety reasons is also ensured in case of
– impacts by flotsam,
– consequences from ship accidents, and
– collisions of ships with cooling water structures

according to the site-specific requirements.

3.2.2.1 (2) The effects of ship accidents on the quality of the cooling water, e.g. by admixture of oil or other dangerous substances, is taken into consideration.

3.2.2.2 Electromagnetic impacts (except lightning)

3.2.2.2 (1) Relevant electromagnetic interference outside the plant are identified and the potential impacts resulting from it are assessed. The consideration of enveloping impacts is permissible. An electromagnetic compatibility (EMC) analysis is performed to the required extent.

3.2.2.2 (2) As far as electromagnetic influences may impair the function of safety-relevant installations, measures and installations are provided for protection of their I&C according to their safety significance.

3.2.2.2 (3) For safety-relevant installations that may be impaired by electromagnetic impacts, it is demonstrated by tests that their electromagnetic compatibility is given in their application environment (verification of EMC compatibility).

3.2.2.2 (4) During the lifetime of the plant, the protection of safety-relevant installations against electromagnetic influences is being adapted to changed environmental conditions, if any.

3.2.3 Natural events

3.2.3.1 Lightning

3.2.3.1 (1) It is ensured that structures and safety-relevant electrical and I&C components are not impaired by lightning in an undue manner.

3.2.3.1 (2) The lighting protection includes structural measures a n d / o r other installations (such as armouring) as well as measures and installations for the protection against other electromagnetic influences.

3.2.3.2 Earthquake

3.2.3.2 (1) For the site, the design earthquake and the associated impacts are determined on the basis of the results of deterministic and probabilistic analyses.

As characteristic parameters of the design earthquake, site intensity, ground respond spectra and strong motion duration are specified.

Irrespective of the site-specific specifications, the design is at least based on the intensity VI EMS/MSK.

3.2.3.2 (2) It is ensured by the design of plant structures, systems and components as well as other measures and installations that the protection goals are fulfilled in all operating phases.

3.2.3.2 (3) Here, underground changes (e.g. soil liquefaction or settling) are also taken into consideration in addition to vibratory excitation of structures, systems and components.

3.2.3.2 (4) For the reactor coolant pressure boundary and the external systems required for the fulfilment of the protection goals, the behaviour during design earthquakes is assessed by means of a structure-dynamic analysis and the fulfilment of the protection goals ensured. Simultaneous overlapping of the impacts from earthquake and a leak in the reactor coolant pressure boundary is not postulated due to its design and construction. Simultaneous overlapping of a leak in the external systems is not postulated if these are designed against earthquake.
N o t e: See "Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System" (Module 4), Section 2, 3 and 5.

Irrespective of it, it is ensured that the shutdown systems, the emergency and residual-heat removal systems, the containment system as well as the control room remain operable also in case of the design earthquake.

3.2.3.2 (5) Seismic instrumentation is available by means of which the engineering seismological parameters of relevant earthquakes can be determined.

The seismic instrumentation is able to display the excess of limit values for the inspection level of the plant as well as to enable a comparison between the design spectrum of the plant and the response spectra of registered earthquakes.

3.2.3.2 (6) The plant operating procedures define limits of the seismic loads where plant controls and, if required, measures (e.g. plant shutdown, determination of the plant condition) shall be initiated if these are exceeded. It is ensured that the relevant values from the seismic instrumentation are available to the operating personnel.

3.2.3.2 (7) Combinations of earthquake impacts with earthquake-induced consequential impacts (burst pressure blast waves due to failure of vessels with high energy content, missile impacts, fires, floods) are taken into consideration.

3.2.3.3 Flooding

3.2.3.3 (1) External flooding does not impair plant safety in an undue manner.
The possible causes for flooding are considered site-specifically.

3.2.3.3 (2) Regarding external flooding events, a design flood level is defined for the design flood. The plant is designed accordingly.

3.2.3.3 (3) Besides the static impact by the water pressure, potential dynamic effects (such as wash of waves or flotsam impact) are considered in the design of permanent or temporary installations that prevent intrusion of water into safety-relevant buildings.

3.2.3.3 (4) Consequential impacts of flooding are considered.

3.2.3.4 Extreme meteorological conditions

3.2.3.4 (1) Measures and installations are provided such that extreme meteorological conditions do not lead to safety-relevant impacts on the plant and the function of its safety-related installations. In this respect, the plant operating procedures define within which limits plant operation is permissible and how to proceed if the limits defined are exceeded.

3.2.3.4 (2) The extreme meteorological conditions considered site-specifically are, in particular,
- high and low temperatures (outside air and cooling water), including consequential effects, such as increased condensate accumulation,
- long-lasting drought and its impact on cooling water supply,
- storm,
- mudslide, landslide,
- high and low humidity,
- snowfall,
- icing,
- hail,
- thunder storm, and
- salt deposits on electrical insulators.

3.2.3.4 (3) The possibility of a failure of supply units (e.g. freezing of supply pipes or operating materials) is considered.

3.2.3.4 (4) In particular, measures and installations are provided against icing in the area of the safety-relevant installations, such as cooling water intake, air supply devices or pressure relief systems.

3.2.3.4 (5) Measures and installations are provided against impacts by storms. Here, the following aspects are considered in particular:
- wind force,
- turbulence,
- total impact duration,
- interaction with neighbouring structures,
- wind-induced receiving water level, and
- wind-blown or falling objects and equipment.

3.2.3.5 Biological impacts

3.2.3.5 (1) For the relevant impacts occurring at the site, measures and installations are provided to prevent safety-relevant impacts. Here, consequential impacts, such as microbiological corrosion, are also considered.

3.2.3.5 (2) The receiving water is regularly monitored with regard to a change of the biological conditions.

3.2.3.5 (3) Measures and installations are provided against harmful effects of vegetable matter and organisms in the cooling water and service water system (e.g. undue impairment of the heat exchanger surfaces) and against the accumulation of vegetable matter or organisms in front of the cleaning systems (e.g. rack or travelling screen). Where appropriate, the cooling water is treated with regard to the prevention of harmful effects.

3.2.3.5 (4) Blocking of safety-relevant systems for air and water supply is prevented by appropriate measures and installations.

3.2.3.5 (5) Safety-relevant systems for air supply or water intake can be cleaned easily.

4 Criteria for measures and installations in case of whose existence occurrence of specific events is not postulated (preventive measures)

N o t e: According to the "Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors" (Module 3), subsection 1 (3), for some events there is the option to demonstrate that due to preventive measures the occurrence of these events is so unlikely that they do not have to be postulated. In the "Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors" (Module 3), these events are classified as VM *(German abbreviation for Vorsorgemaßnahme = preventive measure).*

4.1 General criteria

4.1 (1) Reliability and effectiveness of the preventive measure(s) are such that occurrence of the event does not have to be postulated.

The quality of the preventive measures to be taken is oriented towards the potential impacts.

4.1 (2) Preventive measures are mainly based on passive installations. If this cannot be realised, reliable active installations are available.

If the reliability criteria according to subsection 4.1 (6) have been demonstrated, administrative measures can also be referred to.

If in the exceptional case preventive measures are exclusively based on administrative measures, their reliability is justified specifically.

4.1 (3) The totality of the preventive measures ensures the effectiveness of these measures also in case of a single failure.

4.1 (4) During the performance of maintenance measures including in-service inspections, reliability and effectiveness of the preventive measures will not be impaired in an undue manner.

4.1 (5) Preventive measures are designed such that they do not impair the operability of safety-relevant plant components in case of malfunction or damage to them or in case of operator error/human error.

4.1 (6) If administrative measures and personnel actions derived from them are comprised in preventive measures, their effectiveness and reliability is demonstrated by methods such as failure mode and effects or hazard analysis. In particular, systematic failures are taken into consideration.

The following conditions are ensured:

a) Clear organisational specifications are defined regarding competence and responsibility for the measures. The personnel entrusted with the performance and control of preventive measures is especially qualified for their performance and control in accordance with the high requirements regarding the reliability of such measures.
b) There are clear procedures and clear instructions for the performance and control of the measures. Type and number of the control measures are defined in accordance with the requirements regarding the reliability of the respective measure. For the control of success, clear, i.e. measurable and quantifiable criteria are defined. The proceeding in case of deviations identified is defined.

c) The measures are fully documented. Here, the individual steps of performance and the control measures are clearly traceable and the persons involved stated.
d) There is sufficient time available for the performance of the work steps and control of the measures.
e) The environmental conditions do not impair the performance and control of the measures.
f) The boundary conditions under which the persons in charge of the performance of the measures are designed such that the prerequisites for a behaviour as failure-free as possible are given. The ergonomic criteria according to Section 6.3 are considered.
g) Potential failures and their consequences are considered in the training of the personnel.

4.1 (7) The validity of the boundary conditions for effectiveness and reliability of the preventive measure is ensured during the entire lifetime of the plant.

4.2 Event-specific criteria

4.2.1 Entry of unborated water or low-borated coolant into the reactor core

N o t e: This comprises the PWR events E3-17 “Inadvertent injection from a system carrying unborated water or low-borated coolant with loss of limitation systems or preceding procedures (external boron dilution; homogeneous and heterogeneous) and E3-18 “Formation of low-borated areas in the primary circuit (internal boron dilution) according to the “Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors“ (Module 3).

4.2.1 (1) Measures and installations are provided to ensure that reactivity changes due to the entry of unborated water or low-borated coolant into the reactor core remain limited to such values with which,
- for an initially critical reactor, the safety-related acceptance target for the reactivity-initiated accident according to the “Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors“ (Module 3), Table 3.1, and
- for an initially critical reactor, the required contribution of the shutdown reactivity according to the “Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors“ (Module 3), Table 3.1,

are maintained.

4.2.1 (2) Potential sources for an entry of unborated water, the potentially entered amounts of unborated water and the potential impacts on the reactor core are analysed for all operating phases. Here, the following sources of unborated water are considered in particular:
External sources:
- All systems connected to the reactor coolant system that contain unborated water,
- heat exchanger leakages (steam generator, aftercooler),
- low-borated media in adjacent systems and vessels.

Internal sources:
- boron removal from the coolant during “small leak (reflux condenser operation),
- shutdown during natural circulation and with secondary-side isolated steam generator.

4.2.1 (3) The analysis considers operating errors.

4.2.1 (4) Impermissible entry of unborated water from external sources is prevented, e.g., by the following measures and installations:
- Reliable closure and interlocking of all valves through which unborated water may inadvertently enter the reactor coolant system,
- monitoring of the boron concentration in adjacent systems and components and
- automatic continuous monitoring of the boron injection concentration.

4.2.1 (5) Inadvertent start of main coolant pumps after previous reflux-condenser operation is reliably prevented according to Section 4.1.

4.2.2 Drop of a fuel element into the reactor core during refuelling (BWR) Inadvertent withdrawal of control rods during core loading (BWR)

4.2.2 (1) Measures and installations are provided so that the drop of a fuel element into the reactor core does not lead to criticality.

4.2.2 (2) Measures and installations are provided that prevent unplanned withdrawal of control rods during loading of the reactor and allow loading only if all rods are inserted.

4.2.3 Misloading of the reactor core, of the fuel pool or of the transport and storage cask with more than one fuel element

Preventive measures are taken that
- prevent misloading of the reactor core, of the fuel pool or the transport and storage cask with more than one fuel element reliably according to Section 4.1, or
- ensure that in case of such misloading, the required subcriticality is maintained.

4.2.4 Leak/break in main steam or feedwater system and other high-energy piping systems in the annulus and in the valve compartments (PWR) and between containment and first isolation possibility outside the containment (BWR)

The impacts of leaks in the annulus and in the valve compartments (PWR) and in the area between containment and the first external isolation possibility (BWR) in piping systems carrying main steam or feedwater, in a steam generator blowdown line (PWR) or on another high-energy pipe are limited or controlled such that undue impairment of the containment, including the penetrations, as well as of safety-relevant installations in the area between containment and reactor building (annulus) and in the valve compartments (PWR) is not to be postulated.

Impermissible impacts are prevented or controlled, e.g., by appropriate design of the pipes in this area or by guard pipe constructions.
N o t e: Specific relevant criteria are to be found in “Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System“ (Module 4), Section 4.6 and 6.

4.2.5 Loss of tightness between drywell and wetwell (BWR)

Preventive measures are taken so that no impermissible leaks between drywell and wetwell, in particular during restart of the plant and after maintenance measures, exist or can occur.

5 Specific criteria for structures, systems and components
N o t e: For the structures, systems and components the requirements of the Equipment and Product Safety Act (GPSG), the Ordinance on Industrial Safety and Health (BetrSichV) and the Pressure Equipment Ordinance (14^{th} GPSGV) are also applicable.

5.1 Criteria for structures (buildings)

5.1 (1) According to their safety significance, the structures withstand the impacts to be postulated with sufficient reliability. They remain, according to the safety criteria they have to fulfil, in a condition suitable for use or at least in a condition with sufficient load-carrying capacity. For fulfilment of the safety-related functions, required limits for deformation and crack width are adhered to in addition to maintenance of the load-carrying capacity.

5.1 (2) The safety significance and the design of structures result from their function regarding the maintenance of the operability of safety-relevant installations and their direct contribution to the fulfilment of the protection goals regarding events on levels of defence 2 to 4a.

5.1 (3) All structures are classified according to their safety significance as stated in the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1), subsection 2.1 (10).

5.1 (4) As basis for the structural design, all impacts on the structures are described and quantified such that they can be used as clear specification for the dimensioning and construction of structures including their anchorings for components. The design considers potential ground settlement, subsidence damages, etc.

5.1 (5) Combinations of impacts with the associated rated values are postulated if these may be causally connected or if their simultaneous occurrence has to be postulated according to probability considerations or the state of the art in science and technology. Consequential impacts are considered

N o t e: See also in the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1), subsection 4.1 (5) and in the “Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation" (Module 6), Section 3.2.1 and subsection 3.2.4 (7), 3.2.4 (8 and 3.2.5 (4).

5.1 (6) The loads resulting from interactions at the interface between structure and component are safely applied to the structure by anchoring/attachment constructions and transferred by them. The loads resulting from interactions at the interface between structure and component are determined for the interface between anchoring and component.

5.1 (7) The mutual impermissible influences of buildings is avoided.

5.1 (8) Settlement of the structures does not have the effect that the suitability for use of the structures or the function of safety-relevant systems is impaired. For cable and pipe laying, the differential settlements between the structures are considered.

5.1 (9) Safety-relevant structures are protected against water intrusion from outside by adequate sealing measures. For this purpose, waterproof constructions or external waterproofing of structures are provided. Waterproofing of structures is, in particular, designed against impacts resulting from groundwater, flood, earthquake and plant-internal events, including ionising radiation.

5.1 (10) For the retention of radioactively contaminated liquids, external waterproofing is not taken into account at levels of defence 1 and 2. For events on level of defence 3, the presence of a functioning external waterproofing, where applicable in addition to the internal retention function, may be considered regarding the leakage of radioactively contaminated liquids.

5.1 (11) With regard to dimensioning and selection of the construction materials, the structures are designed such that they ensure a shielding function that meets the requirements of radiation protection.

5.1 (12) Surfaces in rooms in which contamination is to be expected are designed such that they can be easily decontaminated.

5.1 (13) In rooms where operation-induced leakages may occur, floor drains are installed.

5.1 (14) The structures meet the requirements posed during their entire service life.

5.1 (15) Testing and monitoring measures, at least regular walk-downs and visual inspections of structure surfaces are provided. The results are documented. At intervals of ten years, a report is prepared on the condition of the structures. In case of indications, investigations are conducted on the cause and, where required, proper repair is performed.

5.2 Component-specific criteria

N o t e: Specific criteria for the reactor coolant pressure boundary, the pressure-retaining walls of components of the external systems and the containment system are to be found in “Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System“ (Module 4).

5.2.1 General criteria

5.2.1 (1) The safety-relevant components fulfil the criteria at those levels of defence according to which they are allocated.

5.2.1 (2) All relevant impacts on the components due to mechanical and thermal impacts, corrosion and erosion are considered in the design, construction and calculations.

The surfaces of metallic components fulfil the criteria regarding corrosion prevention and, where necessary, ease of decontamination. The surfaces of austenitic materials are protected against contact with ferritic materials or agents containing chloride from construction and operation of the plant.

5.2.1 (3) The boundary conditions, in particular of radiation protection, resulting from the performance of maintenance measures are considered.

5.2.1 (4) Components are classified according to the “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1), subsection 2.1 (10) and, as far as necessary, labelled systematically.

5.2.1 (5) The design of the structures systems and components is based on load cases, beginning with impacts. The load cases are derived, in particular, from specified plant operation, from operating experience and from the events postulated according to the “Safety Criteria for Nuclear Power Plants. Events to be considered in Pressurised and Boiling Water Reactors” (Module 3) and cover the resulting impacts. The load cases and their combinations are specified and completely described according to their characteristics and frequency. Load case combinations are postulated if the events a n d / o r operating phases to be combined may be causally connected or if their simultaneous occurrence has to be postulated according to probability considerations. The impacts resulting from these load cases are described component-specifically also under consideration of the technology of adjacent systems.

5.2.2 Criteria for support structures, hangers and walk platforms

N o t e: Among the installations to be considered here are supports, suspensions, cable racks, pipe whip restraints, crane runways, platforms and protective structures.

5.2.2 (1) Support structures, hangers and walk platforms are capable of applying the specified loads to the load-transferring building structure.

5.2.2 (2) The impact collective and the resulting loads on the support structures, hangers and walk platforms are fully known and considered in the design of these installations. It includes
- specific weight,
- operational loads,
- hoist loads,
- building settlements,
- test loads,
- assembly loads,
- internal impacts (radiation, temperature, humidity, impact loads, jet and reaction forces), and
- external impacts (induced vibrations, impact loads).

5.2.2 (3) Movable parts of hangers (e.g. spring hangers, shock suppressors, dampers) are subjected to in-service inspections. Rigid components are subjected to regular visual inspections or, where appropriate, to non-destructive tests.

5.2.2. (4) Temporarily assembled platforms and support structures are secured such that they do not lose their stability due to operating conditions and events on levels of defence 1 to 4a or that the loss of stability does not lead to impermissible impacts.

5.2.2 (5) The drop of components during assembly and disassembly of the temporary installations as well as the drop of parts stored on them during the service life of these installations is considered.

5.2.3 Criteria for electric drives

N o t e: See also “Safety Criteria for Nuclear Power Plants: Criteria for Electric Power Supply (Module 12).

5.2.3 (1) The electric drives fulfilling functions at levels of defence 1 to 4 perform their tasks also under the environmental conditions, process-related loads and electrical conditions to be postulated.

5.2.3 (2) The protection equipment of the electric drives (e.g. against overvoltage, undervoltage, overload) are aligned with the drives and the electric power supply to be protected such that both the components are reliably protected and that there is sufficient margin to the most unfavourable operating values of the electric supply. The response of protection equipment is signalled.

5.2.3 (3) Installations of the equipment unit protection are designed such that in case of actuation of electric drives by the instrumentation and control equipment of the safety system, the equipment unit protection will on principle not become effective (for further details, see “Safety Criteria for Nuclear Power Plants: Criteria for Instrumentation and Control and Accident Instrumentation“ [Module 5], subsection 3.2 (13)).

5.2.3 (4) For valve drives, the reduction of power, moment or force due to self-heating, increased environmental temperature and voltage drop is considered up to the drive for the respective case of challenge.

5.2.4 Criteria for valves

N o t e: Criteria for electric drives are included in Section 5.2.3.

5.2.4 (1) If valves are part of the reactor coolant pressure boundary, part of the pressure-retaining walls of the external systems or of the containment system, the criteria of “Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System“ (Module 4) are fulfilled.

5.2.4 (2) All parameters relevant for the function of valves according to the requirements, such as loads, stresses, friction and material properties, are considered such that the function is ensured with sufficient safety distance also in case of combination of the variation ranges of individual parameters. Here, support and storage are also considered.

5.2.4 (3) For valves that have to close against the maximum possible pressure difference under the respective conditions, the operability is demonstrated by analytical demonstration as well as by appropriate tests.

5.2.4 (4) In the event of a valve shut-off failure, the integrity of safety-relevant valves is maintained. Any further safety-related criteria (e.g. on the operability) are specified in the individual case.

5.2.4 (5) For system-medium operated valves, measures and installations are provided against a failure due to a common-mode failure in the valve control. Here, the single failure concept is applied to all elements of the pilot equipment.

5.2.5 Criteria for overpressure protection and pressure relief of the reactor coolant system and the main steam system

N o t e: For the plant components dealt with in the following, in particular, the requirements of the Pressure Equipment Ordinance (14th GPSGV) are also applicable.

5.2.5.1 General criteria for overpressure protection and pressure relief

5.2.5.1 (1) The devices for overpressure protection ensure that in case of events on levels of defence 2 to 4a, the maximum allowable stresses of the systems and components to be protected according to the “Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors“ (Module 3) are not exceeded.

5.2.5.1 (2) The devices for overpressure protection open and close reliably under the conditions on levels of defence 2 to 4a taken as a basis.

5.2.5.1 (3) The states of the medium to be discharged that may result from the events on levels of defence 2 to 4a to be controlled by the devices for overpressure protection are considered.

N o t e: Criteria regarding levels of defence 4b and 4c, see in “Safety Criteria for Nuclear Power Plants: Criteria for Accident Management“ (Module 7).

5.2.5.1 (4) The valves are qualified regarding the respective blowdown conditions to be expected (e.g. states if matter).

5.2.5.1 (5) For boiling water reactors and the secondary side of pressurised water reactors, sufficiently reliable pressure relief devices are provided. These are able to reduce the main steam or reactor pressure in a controlled manner automatically or manually within specified time limits to sufficiently low values according to the respective level of defence.

5.2.5.1 (6) Devices for pressure limitation are regularly subjected to functional tests. The test concept ensures that the operability can be assessed over the entire maintenance interval of a device.

5.2.5.1 (7) Functional tests on overpressure protection devices of activity-retaining systems do not lead to a release of radioactive material into the building atmosphere.

5.2.5.2 Specific criteria for overpressure protection in pressurised water reactors

5.2.5.2 (1) Relief valves are equipped with a pre-closing, which closes automatically when the valve is stuck open inadvertently. In order to exclude inadvertent closure of devices for pressure limitation, installations are available that assume the pressure limitation function in case of inadvertent closure independent of the relief valves (and their actuation).

5.2.5.2 (2) The response pressure of the devices for pressure limitation of the reactor coolant system is adapted to the temperature level of the system to be protected for prevention of brittle fracture.

5.2.5.2 (3) For events on level of defence 2 with actuation of reactor scram, the response pressure of the pressuriser safety valves is not reached.

5.2.6 Criteria for pumps

N o t e: For pump casings being part of the reactor coolant pressure boundary or assigned to the scope of application of the "Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System" (Module 4) for other reasons, the criteria mentioned there are applicable.

5.2.6 (1) Criteria from operation and environmental conditions

a) In addition to the process-related criteria, the design of the pumps considers the following conditions:
- mechanical loads (such as pressure differences),
- environmental conditions (e.g. temperature, humidity, radiation),
- different operating modes (continuous, discontinuous),
- the medium to be conveyed (including pH value, dirt content, viscosity),
- the minimum flow rate,
- cooling and lubrication,
- postulated events, such as flooding, earthquake,
- explosion protection,
- radiation protection, including ease of decontamination and tightness, and
- maintenance.

b) Regarding the influences of the connected systems, the design considers the following:
- Vibration transmission to the pumps,
- intake conditions and operating points,
- pressure conditions, pressure surges,
- backflow, and
- torque impact on the nozzles, and
- bearing and fixing for bearing of the loads acting.

c) Pressure oscillations induced by pump operation are reduced to a permissible extent by adequate measures and installations.

5.2.6 (2) Drive units

N o t e: General criteria for electric drives are included in Section 5.2.3.

a) The drive units are qualified for the environmental conditions. They have the required power output and the torques required during start and maximum power. Vibration transmission from the pump is considered. Bearing and fixing of the drive units are designed accordingly
b) If steam turbines or diesel engines are used as drive units, the criteria for these components are considered.

5.2.6 (3) Gear and coupling

a) Gear and coupling transmit the required torques in a reliable manner.

b) Gear and coupling, including cooling and lubrication, fulfil their function under the environmental conditions to be expected.

5.2.6 (4) Operation monitoring
Pumps are provided with devices by means of which in particular the following parameters can be monitored, as far as required:
– Pump pressure,
– suction pressure,
– flow rate,
– temperatures of motor, lubricants and cooling media, as well as
– vibrations.

5.2.7 Criteria for heat exchangers

N o t e: If the heat exchangers are part of the reactor coolant pressure boundary or part of the pressure-retaining walls of the external systems, the criteria of the "Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System" (Module 4) are also applicable.

5.2.7 (1) Heat exchangers fulfil the safety-related criteria with regard to power transmission and barrier and retention function under all boundary conditions specified. Here, the boundary conditions in connection with maintenance measures (e.g. heat input in case of isolated cooling water side) are particularly considered, in addition to the normal operation, anticipated operational occurrences and incidents.

5.2.7 (2) The design of heat exchangers considers the relevant mechanical and thermal loads, in particular fast (dynamic) mechanical and thermal as well as cyclic stresses.

5.2.7 (3) A monitoring programme is provided for ensuring the parameters relevant for power transmission. Continuous monitoring of the relevant parameters is particularly provided for heat exchangers where discontinuous external (e.g. entry of foreign particles, discontinuous pollution effects) may occur. Here, incident-induced impacts are also considered (e.g. entry of insulating material in case of loss-of-coolant accidents).

5.2.7 (4) It is ensured that in heat exchangers no media or foreign matter can accumulate that impair the safety-relevant heat transport or the integrity of the heat exchanger surface in an undue manner. Here, the special conditions in case of incidents are also considered.

5.2.7 (5) Heat exchangers which have a safety-relevant retention function in addition to the function of power transmission are monitored for leakages between the circuits. Allowable leakage rates are specified in the plant operating procedures.

5.2.7 (6) The condition of the heat exchanger tubes is monitored within the framework of the maintenance programme under consideration of relevant damage mechanisms.

5.2.8 Criteria for pipes and vessels

N o t e: If pipes and vessels are part of the reactor coolant pressure boundary, part of pressure-retaining walls of the external systems or the containment system, the criteria of the "Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System" (Module 4) are also applicable.

5.2.8 (1) Pipes and vessels reliably fulfil the safety-related criteria regarding the confinement of radioactive materials and regarding the pressure-retaining components under all boundary conditions specified.

5.2.8 (2) Pipes and closed vessels are protected against undue internal pressures.

5.2.8 (3) In addition to the loads from internal pressure, dynamic loads, such as forced oscillations and thermal expansion, are considered.

5.2.8 (4) The boundary conditions resulting from the performance of maintenance measures are considered.

5.2.8 (5) Laying and layout of pipes and vessels are such that filling, venting and drainage is possible and condensation and water hammers cannot occur. If this cannot be precluded with sufficient reliability, these impacts are considered.

5.2.8 (6) The criteria for internal and external surfaces, such as ease of decontamination, corrosion and wear protection, are fulfilled.

5.2.8 (7) The ageing behaviour is particularly monitored with regard to plastic pipes and coated pipes and vessels.

5.2.8 (8) Buried pipes and vessels do not lose their tightness due to ground settlements. Their location is documented.

5.2.9 Criteria for lifting equipment and load attaching points

N o t e: Both stationary and temporarily used (mobile) elevators, cranes, winches, trolleys, load-bearing equipment and refuelling machines are referred to as lifting equipment, provided such equipment is used in nuclear power plants.

The load attaching point is the connecting element between load suspension device and load and is either
a) an integral part of the load, or
b) bolted on, or
c) welded on, or
d) anchored in the concrete in the case of structural concrete components.

5.2.9 (1) At a nuclear power plant, lifting equipment is provided which, in interaction with the load attaching points and the attachment devices, ensures that during the handling of loads during specified normal operation under consideration of the maximum mechanical, thermal, chemical or radiation-induced impacts resulting from it the protection goals are adhered to.

5.2.9 (2) The safety-relevant function of the lifting equipment is ensured with sufficient reliability by corresponding dimensioning and construction, selection of adequate materials, ergonomic design and, where required, by redundant design of I&C equipment and auxiliary and supply systems.

5.2.9 (3) The reliable function of the lifting equipment and load attaching points is ensured for the entire lifetime of the equipment by regular tests.

5.2.9 (4) The design of lifting equipment and load attaching points considers the environmental conditions to be expected, such as pressure, temperature, medium and radiation exposure.

5.2.9 (5) The criteria regarding ease of decontamination of the lifting equipment in the controlled area are considered in the structural design.

5.2.9 (6) If, in the course of transportation of nuclear fuel, other radioactive substances, radioactive components or other loads, a failure of the lifting equipment or of load attaching points is expected to lead
a) to an activity release which may lead to an undue radiation exposure in the plant or the environment,
b) to a loss of reactor coolant which cannot be isolated,
c) to a redundancy-wide impairment of safety installations which is necessary to fulfil the protection goals, or
d) a criticality event,

then, the cranes, winches, trolleys, load-bearing equipment, attachment devices, load attaching points and refuelling machines are designed such that load-drop, roll-over or hitting with undue consequences is not to be postulated (see Section 2.2.4).

5.2.9 (7) For external events, the following criteria are fulfilled:
a) Adequate protection of lifting equipment against external events (events on level of defence 3 or 4a) is demonstrated, provided such requirement exists for the building. The safety demonstration includes the integration into the building.
b) The adequacy of the protection against external events can be demonstrated for the lifting equipment without load if it is ensured that loads and load-bearing equipment are only attached to the lifting equipment during the period required for the lifting process.

c) If lifting equipment exclusively remains in one parking position during defined operating phases, at least one demonstration of protection against external events in these operating phases is given which is limited to this position.

5.3 System-specific criteria

5.3.1 Criteria for the emergency core cooling and residual-heat removal system

5.3.1.1 General criteria

5.3.1.1 (1) For heat removal during and after loss-of-coolant accidents, a reliably effective redundant emergency core cooling and residual-heat removal system is available according to “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“ (Module 1), subsection 3.3 (4). It is appropriate for reaching the acceptance targets and acceptance criteria in case of leaks and breaks in the reactor coolant pressure boundary according to the “Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors" (Module 3) specified there.

5.3.1.1 (2) The emergency core cooling and residual-heat removal system is in stand-by position and isolated from the reactor coolant system. Connections of emergency core cooling subsystems via pipes are closed when in stand-by position and reliably isolable when required.

5.3.1.1 (3) The injection of emergency coolant into the reactor coolant pressure boundary is indicated in a reliable manner. The measuring equipment required for this purpose is installed as closely as possible to the points of injection into the reactor coolant pressure boundary.

5.3.1.1 (4) For PWRs, the compartment around the reactor pressure vessel is capable of being flooded at least up to the upper edge of the reactor core if a leak occurs in the reactor pressure vessel.

5.3.1.2 Ensuring sufficient emergency coolant inventory

5.3.1.2 (1) For PWRs, the emergency coolant inventory is dimensioned such
a) that, when demanded, additional coolant can be injected by means of the high-pressure injection system as long as the primary circuit has reached a pressure level, by corresponding measures (e.g. secondary-side cooling of the primary systems), at which injection of additional coolant is possible by means of the low-pressure injection system,
b) that after injection of the emergency coolant inventory, assured suction of the low-pressure return flow from the containment sump is possible and heat removal is ensured in the long term also in case of the most unfavourable leakage under consideration of dead volumes in the containment.

5.3.1.2 (2) For BWRs, the emergency coolant inventory is dimensioned such that additional coolant can always be injected to the required amount, assured suction of the low-pressure return flow from the containment sump is possible under consideration of the dead volumes and heat removal is ensured in the long term.

5.3.1.2 (3) In case of leaks in the emergency core cooling and residual-heat removal system (PWR and BWR) at any point outside the containment, the available water supply remains to be sufficient for emergency core cooling purposes.

5.3.1.3 Design criteria for components of the emergency cooling systems and the containment

5.3.1.3 (1) The permanent operability of the emergency core cooling and residual-heat removal systems is not unduly impaired by system contamination with particulate and foreign matter (in particular insulation material).

Heat removal from the reactor core is not unduly impaired by material entry during sump operation either.

5.3.1.3 (2) For PWRs, the characteristic of the high-pressure injection system is defined such that the core can be covered by coolant injection in the long term, also at a maximum primary-side saturation pressure to be postulated after reactor scram, due to a reliable secondary-side heat removal.

5.3.1.3 (3) The active components of the residual-heat removal systems relevant for effectiveness can be maintained during the long-lasting heat removal process.

5.3.1.3 (4) The design of the containment and its internals ensures that in case of a loss-of-coolant accident the coolant leaking out of the break gets into the containment sump (PWR, BWR) or into the wetwell (BWR) to a sufficient amount according to subsection 5.3.1.2 (1) b) to ensure operation of the residual-heat removal pumps without cavitation.

5.3.1.3 (5) The emergency core cooling system is designed such that in case of a loss-of-coolant accident a long-term temperature or pressure increase in the containment after refilling of the core during sump operation is prevented (see “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria“[Module 1], subsection 3.6 (2)).

5.3.1.4 Criteria for the secondary-side heat removal

For the control of design basis accidents requiring secondary-side heat removal, the following assumptions are made or design conditions fulfilled:

– Components and systems required for secondary-side heat removal (e.g. auxiliary feedwater pumps, secondary-side blowdown station as well as its activation circuits) are considered as subsystems of the emergency core cooling and residual-heat removal system.
– The water supply for emergency injection is dimensioned conservatively regarding the design basis accidents to be postulated. The water supply is sufficient for the removal of the decay heat for 10 hours (emergency conditions) and the subsequent shutdown, including the removal of storage heat. Water supplies that might be required additionally for room and / or component cooling are considered in the calculation of the water supply.

5.3.2 Criteria for emergency systems for man-made hazards

5.3.2 (1) In case the control room is not operable, it is ensured that the emergency systems for man-made hazards will bring the plant into a controlled plant condition without any manual intervention and that the plant can remain in this condition for at least 10 hours. In addition, it is possible, with the aid of these emergency systems, to bring the plant into a condition which ensures subsequent residual-heat removal through the emergency residual-heat removal system in the long term.

5.3.2 (2) In detail, the emergency systems for man-made hazards comply with the following criteria:

a) Components and subsystems of these emergency systems are especially protected against external events.
b) It is ensured that the function of these emergency systems cannot be unduly impaired by damages in plant areas which may be destroyed. This applies not only to process systems but also to energy supply systems and I&C installations.
c) It is ensured that unauthorised interventions or maloperations in the control room or in other plant areas which are not especially protected cannot lead to any undue impairment of the function of these emergency systems.
d) No interventions in these emergency systems are made, be it for operational reasons or testing purposes, if such interventions cannot be made undone or completed in case of an emergency and will lead to an undue impairment of the function of the measures or systems. This does not apply if equivalent functions are provided.

5.3.2 (3) The cooling of the fuel elements in the long-term residual-heat removal phase under the man-made hazard conditions “aircraft crash” and “explosion blast wave“ is ensured. At the installations required for this phase, repair measures can be performed in time, if required.

5.3.2 (4) The accessibility of areas where operations might have to be performed locally as well as the communication with the personnel working there are ensured.

5.3.3 Criteria for ventilation systems for room air conditioning

N o t e: Criteria concerning radiology are dealt with in "Safety Criteria for Nuclear Power Plants: Criteria for Radiation Protection" (Module 9).

5.3.3 (1) The nuclear power plant has reliable and effective ventilation systems for the following rooms:

- Rooms in which the values for room air conditions specified as permissible for the different levels of defence (e.g. subatmospheric pressure) cannot be adhered to in any other way, or in which installations of safety significance requiring air cooling are located.
- Rooms in which the air is substituted by an inert gas or in which, for reasons of work protection and the ability of persons to perform actions, specific room air conditions must be adhered to.

5.3.3 (2) The ventilation systems are designed, conditioned and matched with the features of the other systems such that at the levels of defence 1 to 4a the respective values for the room air conditions specified as permissible are adhered to.

5.3.3 (3) The ventilation systems are designed and conditioned such that for events on level of defence 4a they ensure adequate protection against entry of hazardous materials according to Section 3.2.1.4 and the effects of explosion blast waves.

5.3.4 Criteria for the pressure suppression system (BWR)

5.3.4 (1) The design of the pressure suppression system considers all loads from the levels of defence 1 to 4a (in particular, also the dynamic loads). The containment, consisting of drywell and wetwell is designed such that the function of the wetwell regarding pressure suppression and relief is ensured without consideration of the suppression pool spray system. The tight sealing between drywell and wetwell is ensured.

5.3.4 (2) Within the wetwell, there are no components whose failure might impair the operability of the pressure suppression system.

5.3.4 (3) The shut-off devices in the connections between wetwell and drywell automatically and reliably close after pressure equalisation has been reached and sufficient tightness is given. Their tightness can be checked. The shut-off devices provided for pressure equalisation after loss-of-coolant accidents are not actuated in case of pressure equalisation processes during normal operation.

5.3.4 (4) Condensation and clearing processes do not cause any impermissible impacts.

5.3.4 (5) The operability of the pressure suppression system is demonstrated by tests.

5.3.4 (6) It is demonstrated that, compared to the wetwell, no negative pressure can occur in the drywell after loss-of-coolant accidents which endangers the wetwell, its function or the steel liner and its anchoring.

5.3.4 (7) It is ensured that no impermissible building vibrations are induced by actuations during loss-of-coolant accidents or by blowdown processes.

5.3.5 Criteria for the possibilities of degassing the reactor pressure vessel

5.3.5 (1) Isolable equipment is provided by means of which gas accumulations in the reactor pressure vessel can be reduced.

5.3.5 (2) The actuation of the valves in the connecting lines is performed manually by remote control. Protection against maloperation is provided. The equipment needed for remotely operated degassing are designed such that they also withstand the ambient conditions during a loss-of-coolant accident.

6 Other criteria

6.1 Criteria for rescue routes and for alarms

6.1 (1) Rescue routes are provided by means of which persons can get into the open fast and safely in case of danger and can be rescued from outside. Further, the secured rescue routes are suitable as access ways for hazard control.

6.1 (2) Rescue routes fulfil the following criteria:
- They are marked in a simple, clearly visible and long-lasting way with a clear escape direction,
- they are equipped with a normal and emergency lighting,
- they offer protection against impact of hazards and ensure reduction of the duration of hazard impacts,
- they are qualified for escape and the transport of injured,
- they offer safe guidance out of the danger zone,
- they allow the transport of hazard control equipment,
- they are equipped with communication means.

6.1 (3) Secured and non-secured rescue routes are regularly controlled for proper condition.

6.1 (4) As a matter of principle, there are redundantly designed alarm systems with optical or acoustic signalling. Signalling takes place within the building or at the plant site.

6.1 (5) The personnel is regularly instructed on the meaning of alarm signals, the behaviour in case of alarms and the use of rescue and personal protection equipment.

6.1 (6) Alarm and rescue exercises are performed at regular intervals. External rescue organisations are involved in the exercises.

6.1 (7) For information of the control room about hazard conditions at the plant and initiation of rescue activities, extension phones with indication of location are installed at the following places:

a) In common rooms, except for rooms for seminars and training, break rooms, rest rooms, rooms for staff on standby and offices,
b) at actuation stations for stationary extinguishing systems,
c) in necessary corridors, especially in the area of entrances to the necessary stairways and to the outside and other exits to the outside,
d) in necessary stairways in the area of direct entrances to accessible rooms as far as no other entrance to the room via a necessary corridor exists.

6.1 (8) Plant-specific and incident-specific criteria are laid down for the kind and time of release of the specified alarms and / or automatic alarms. Necessary personnel actions are planned, if appropriate, with a number of alternatives. For these actions, exercises are performed at least at intervals of six months.

6.1 (9) Measures and installations ensure that the personnel will have sufficient time to escape or will be sufficiently protected under the prevailing conditions if safety valves in the containment respond (in particular, before response of the rupture disk of the pressuriser relief tank).

6.2 Criteria for control room, emergency control room and local control stations

6.2 (1) Operating and plant conditions on levels of defence 1 to 4a are monitored within the respective safety-related scope according to the safety criteria.

Note: Criteria regarding levels of defence 4b and 4c, see in “Safety Criteria for Nuclear Power Plants: Criteria for Accident Management“ (Module 7) subsection 3.3 (6).

6.2 (2) Spatial arrangement, design, shielding, ventilation, lighting and, as far as required, power supply from emergency power system for control room, emergency control room and local control stations are such that, when required, the personnel can stay in them, leave them and access them.

6.2 (3) Necessary measures and installations are provided to ensure a longer-term presence of the operating personnel in the main control room and the emergency control room in the event of an emergency.

6.2 (4) This involves the use of adequate filters for supply air and the possibility of maintaining overpressure in the control rooms to prevent inward leakages.

6.2 (5) The documents required for the performance of the necessary measures are available to the required extent with the possibility of fast access.

6.2 (6) Information are presented such that safety-relevant deviations from specified values can be identified at an early stage.

6.2 (7) With a high information density (signal surge), access to individual safety-relevant technical information remains ensured.

6.2 (8) The plant condition can be determined at the control room, as far as possible, on the basis of different parameters.

6.2 (9) Necessary switching operations for installations fulfilling their functions on levels of defence 1 to 4a can generally be performed from the control room or emergency control room.

6.2 (10) The layout of the operating elements and the indications assigned to them according to function is appropriate and thus they support personnel actions.

6.2 (11) For necessary manual actions of the personnel, simple and clear information and sufficient time are available.

6.2 (12) Alarms with safety relevance are given with high reliability. Hazard alarms are given acoustically and optically.

6.2 (13) Safety-relevant parameters are recorded. The records are archived in a reliable and reproducible manner.

6.2 (14) Malfunctions of systems reported to the local control stations are at least indicated at the control room via group signals.

6.2 (15) The criteria from fire protection and other internal and external impacts are considered in the design of the control rooms.

6.2 (16) The emergency control room can be reached safely. The emergency control room is decoupled from the main control room such that in case of external impacts on level of defence 4a only the main control room or the emergency control room may fail.

6.3 Criteria for the design of the work environment and work equipment

N o t e: On this issue, see also, in particular, the requirements of the Ordinance on Industrial Safety and Health (BetrSichV).

6.3 (1) All foreseeable activities and measures of safety relevance at the plant on levels of defence 1 to 4 are planned under ergonomic aspects such that the prerequisites for optimal behaviour of the persons working at the plant with regard to safety are fulfilled.

This principle applies to the design of all equipment whose use is provided for these activities.

N o t e: The work equipment comprises, among others: information equipment, operating equipment and communication means, measuring and test equipment, tools and other work implements, means of transport, lifting equipment and attachment devices as well as documents with instructions and other information on activities to be performed.

6.3 (2) The principle according to subsection 6.3 (1) applies to the design of all work places where these activities are performed and to the design of the routes used by the personnel to reach the work place with all necessary work equipment.

6.3 (3) The principle according to subsection 6.3 (1) applies to the design of all work environments to whose impacts those performing the activities are exposed to at the work place and on the routes to the work place. This comprises, among others, radiation exposure, lighting and exposure to sonic waves.

6.3 (4) The principle according to subsection 4.3 (1) applies to the design of all work processes, the task sharing between man and technology and the task sharing between those performing these activities.

6.3 (5) The ergonomic design of work environment and work equipment is demonstrated by means of adequate assessment procedures at regular intervals.

6.3 (6) Components that have to be identified for operation and maintenance measures are unambiguously marked.

6.3 (7) The design and modification measures consider the aspects mentioned in subsection 6.3 (1) to (4). Major functional changes at the plant and ergonomic changes at the control room are tested prior to implementation of the modification by means of a simulator. The personnel is trained to the necessary extent prior to implementation of the modification.

K

MODULE 11
"Safety Criteria for Nuclear Power Plants: Criteria for the Handling and Storage of the Fuel Elements"

Contents

1 Objective

This guidance text contains safety-related criteria for the handling and storage of fresh and irradiated fuel elements, also including refuelling, as well as of other core components within the reactor building of a nuclear power plant.

N o t e: A structure is chosen for the guidance text in which initially the criteria are presented that apply in general to the various different areas of handling and storage. There then follow the specific criteria for the dry handling and storage of fresh fuel elements, for the wet handling and storage of fresh and irradiated fuel element, and for refuelling. The criteria are assigned to levels of defence 1 to 4a. As regards levels of defence 4b and 4c, see "Safety Criteria for Nuclear Power Plants: Criteria for Accident Management" (Module 7).

2 Scope

The criteria apply to

a) fuel element handling processes, starting with the acceptance of the fuel elements and ending with their hand-over to the respective transfer points as well as to

b) the dry or wet storage of fuel elements, except for storage in transport and storage casks taking place within the reactor building.

Wherever applicable, the criteria also apply to the handling and storage of other core components, of installations for handling and repair of core components or their parts and of transport and storage casks.

N o t e: A compilation of the events considered in connection with the handling and storage of fuel elements on levels of defence 2 to 4a as well as of the respective safety-related acceptance targets and acceptance criteria is contained in the "Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors" (Module 3) (Table 3.1 to 3.3, Table 5.3 and with regard to refuelling, if relevant, events in the operating phase E from Table 5.1 [PWR] and 5.2 [BWR]).

The installations provided for the handling of fuel elements are dealt with in the "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components" (Module 10).

Criteria with respect to the physical protection of fissile or other materials (security) are set forth in separate regulations.

3 General criteria for the handling and storage of fuel elements in a nuclear power plant

3.1 Level of defence 1

3.1 (1) Measures and installations are provided in the nuclear power plant to handle and store fresh and irradiated fuel elements and further core components as well as fuel element transport and storage casks. During handling and storage, these measures and installations ensure that

a) no undue radiation exposure due to direct radiation will occur,
b) no undue radiation exposure will occur within or outside the plant as a result of an escape of radioactive materials from the fuel elements,
c) the required subcriticality is maintained,
d) fuel cooling is ensured,
e) there will be no mechanical, thermal, chemical or radiation-induced impacts on the fuel elements and the further core components putting their required functional condition or the possibility to store and handle them into question,
f) no damage will occur on the internals of the storage facilities or the reactor pressure vessel.

N o t e: Criteria with regard to the admissible loads on the fuel elements and the further core components are contained in the "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Operation of the Reactor Core" (Module 2), Section 5.

Criteria with regard to the monitoring and limitation of radiation exposure are contained in the "Safety Criteria for Nuclear Power Plants: Criteria for Radiation Protection" (Module 9).

3.1 (2) Each fuel element is clearly identifiable by a visible outside mark.

3.1 (3) Measures and installations are provided with which the fulfilment of the criteria mentioned in subsection 3.1 (1) can be monitored to an appropriate extent during the handling and storage of fuel elements and other core components.

3.1 (4) Measures and installations are provided for the inspection of fuel elements and other core components and for the control of damages.

3.1 (5) Fuel elements and core components are stored in the storage facilities exclusively in the respective positions or areas provided.

The handling of fuel elements and core components is only done in accordance with a quality-assured work procedure, e.g. in the form of a step-by-step schedule.

3.1 (6) For each fuel element, its current storage location, all safety-relevant data as well as any changes in its safety-relevant condition are documented.

The occupation of positions in the storage facility and the reactor core is documented. The documentation is regularly updated.

3.2 Level of defence 2

3.2 (1) The criteria of subsection 3.1 (1) and 3.1 (3) are also fulfilled in the case of the events considered on level of defence 2.

The safety-related acceptance targets and acceptance criteria applying to this level of defence are fulfilled.

3.3 Level of defence 3

3.3 (1) Measures and installations are provided in the nuclear power plant that ensure that for events on level of defence 3 (accidents) which are considered in connection with the handling and storage of fuel elements, the safety-related acceptance targets and acceptance criteria applying to this level of defence are fulfilled.

3.4 Level of defence 4

3.4 (1) Regarding the events considered on level of defence 4a, the safety-related acceptance targets and acceptance criteria applying to this level of defence are fulfilled.
N o t e: Criteria regarding levels of defence 4b and 4c are laid down in the "Safety Criteria for Nuclear Power Plants: Criteria for Accident Management“ (Module 7).

4 Specific criteria for the dry handling and storage of fresh fuel elements

4.1 Level of defence 1

4.1 (1) Measures and installations are provided with which the regular outer condition of the delivered fuel elements and transport casks can be verified.

The regular outer condition of the fuel elements is verified by means of an inspection programme. The relevant condition of the transport cask in this connection is verified as part of the inspection programme. The inspection result is documented.

4.1 (2) To calculate the neutron multiplication factor in the facilities for dry storage (dry storage facilities),
a) the type of fuel element is assumed which under the respective physical and technical conditions will lead to the highest level of reactivity, and
b) the potential moderation and reflection conditions that, taking into account the installations for handling and transport, will lead to the highest neutron multiplication factor are assumed.

4.1 (3) If fresh fuel elements are found to produce a non-negligible output of heat, either sufficient and reliable ventilation is provided or it is demonstrated that the fuel elements will be sufficiently cooled in the dry storage facility even without ventilation.

4.2 Level of defence 2

4.2 (1) The criteria of subsection 4.1 (2) are also fulfilled for the events considered on level of defence 2.

4.3 Level of defence 3

4.3 (1) The criteria of subsection 4.1 (2) are also fulfilled for the events considered on level of defence 3, assuming conservatively moderation with pure water of such a density that will lead to the highest value in the calculation of the neutron multiplication factor in the dry storage facilities in the case of accidents involving changes in moderation.

4.4 Level of defence 4

Regarding events on level of defence 4 there are no criteria beyond those stipulated in Section 3.4.

5 Specific criteria for the wet handling and storage of fresh and irradiated fuel elements

5.1 Level of defence 1

5.1 (1) The installations for wet storage of irradiated and non-irradiated nuclear fuels (spent fuel pools) are housed within sealed buildings in controlled areas.

5.1 (2) The spent fuel pools have sufficient storage capacity. Complete unloading of the reactor core into the spent fuel pools is possible at any time. Here, storage racks that can be inserted into the spent fuel pool in the short term may also be referred to.

5.1 (3) The spent fuel pool is designed such that
a) any harmful effects of the spent fuel pool water on the load-bearing structure of the pool due to leakages can be excluded and that the localisation and elimination of leakages is possible;
b) any leakages from or leaks in the spent fuel pool will only lead to an insignificant drop in the pool water level;
c) any leaks or breaks in connecting piping or component failure in connecting systems or operator errors in connected systems will only lead to a limited drop in the pool water level.

5.1 (4) The installations for making up the water level of the spent fuel pool are designed such that any water losses caused by evaporation and operational leakages are compensated in a way that there will be no interruption of pool cooling due to a drop in the water level.

Installations are available which reliably remove the residual heat from the spent fuel pool in accordance with the requirements, also under consideration of all operating conditions of refuelling and, where required, the simultaneous cooling of the fuel elements in the reactor core as well as during maintenance measures.

5.1 (5) For temporary storage of defective fuel rods, it is ensured that no noteworthy contamination of the cooling water of the spent fuel pool occurs.

5.1 (6) If a spent fuel pool is designed as a multi-zone storage,
a) the maximum number of zones is limited to three;
b) each zone forms a separate unit;
c) the spent fuel pool contains a zone in which also exclusively fuel elements of the most reactive type that are irradiated or which upon the initial presence of burnt-up neutron poisons are in a condition of maximum reactivity under storage conditions can be stored in accordance with the requirements (operative zone);
d) basic minimum burn-up rates of the fuel elements to be stored may be applied for the calculation of the neutron multiplication factors outside the operative zone if it is possible to determine reliably the burn-up-related reactivity effects;
e) incorrect positioning of a fuel element outside the operative zone is prevented by careful planning and quality assurance for the shuffling processes as well as quality-assuring measures during shuffling, high-quality and reliable refuelling machine pre-control devices, optimal ergonomic conditions regarding the handling devices and reliable communication between all those involved;
f) it is ensured that at least two failures or human errors that are independent of each other, becoming effective simultaneously and not to be expected during specified normal operation have to occur before the required subcriticality can be violated.

5.1 (7) For the calculation of the neutron multiplication factors in the spent fuel pools,
a) the type of fuel element is assumed which will lead to the highest reactivity level under the respective physical and technical conditions, and

b) the coolant density possible under the respective conditions and leading to the highest neutron multiplication factor is assumed.

5.1 (8) For the calculation of the neutron multiplication factors in the spent fuel pools, the boric acid dissolved in the coolant within the operative zone may be considered for the PWR if

- the neutron multiplication factor does not exceed the value of 0.98 under normal operating conditions under the assumption of pure water;
- in the event of a reduction of the boric-acid concentration in the water of the spent fuel pool caused by an anticipated operational occurrence or by an accident, boric-acid concentration levels do not – not even locally - fall below the allowed concentration in the area of the storage location.

5.1 (9) If for the PWR the boric acid dissolved in the coolant is considered in the demonstration of the required subcriticality of the spent fuel pool, the boric-acid concentration is monitored with sufficient spatial and time-based resolution. Installations are provided to ensure sufficiently effective boric-acid injection into the spent fuel pool.

5.1 (10) The coolant level is reliably monitored. Undue filling levels are prevented.

5.1 (11) Coolant temperature in the spent fuel pool is reliably monitored. Any undue temperature increases are prevented.

5.1 (12) Coolant temperature in the spent fuel pool is limited so that the rooms around the spent fuel pool are accessible without restrictions and the unrestricted integrity of the spent fuel pool is guaranteed for the entire operating period.

The temperature limits are not exceeded, not even if the spent fuel pool is fully loaded (entire core unloaded).

The calculation of the water temperature is based on the respective most unfavourable conditions regarding residual heat and cooling conditions.

5.1 (13) A water quality is ensured that fulfils the criteria regarding permissible radiation exposure and the maintenance of the safety-relevant characteristics of the fuel elements and the other core components.

The water quality allows sufficient visual checking of the handling processes.

5.1 (14) Measures and installations are provided to prevent reliably the influx into the spent fuel pool of any foreign matter or foreign bodies by which the condition of the spent fuel pool and its safety-relevant installations and of the fuel elements according to the requirements can be impaired.

Foreign matter or foreign bodies that might have fallen in or might have been entrained are recovered or it is demonstrated that leaving them in the system does not raise any safety concern.

5.1 (15) A systems-related link between the emergency core cooling and residual-heat removal system and the spent fuel pool cooling system only exists if it is excluded that disturbances in the pool cooling system cannot demonstrably lead to any noteworthy impairment of the reliability of emergency core cooling and residual-heat removal. The valves that have to be operated to switch over to pool cooling mode are installed outside the containment wherever possible and reasonable.

5.1 (16) If the emergency core cooling and residual-heat removal system is linked to the spent fuel pool cooling system by shared systems, an additional spent fuel pool cooling system train exists which is capable of cooling the spent fuel pool by itself following a loss-of-coolant accident. Wherever possible and reasonable, this system has no active components within the containment. Any valves that have to be operated to start this system up are installed outside the containment wherever possible and reasonable.

5.2 Level of defence 2

5.2 (1) The criteria of subsection 5.1 (7) are fulfilled even in the case of the events to be considered on level of defence 2.

5.2 (2) The safety-related acceptance targets relating to the cooling of the fuel elements are fulfilled even if the spent fuel pool is fully loaded (entire core unloaded).

The calculation of the water temperature is based on the respective most unfavourable conditions regarding residual heat and cooling conditions.

5.3 Level of defence 3

5.3 (1) For the calculation of the neutron multiplication factor in the spent fuel pools under accident conditions,

- the criteria of subsection 5.1 (7) are fulfilled,
- the boric acid dissolved in the coolant may be considered for the PWR if the criteria according to subsection 5.1 (9) are fulfilled.

5.3 (2) For events on level of defence 3 involving a loss of water from the spent fuel pool, measures and installations are provided to detect and stop the loss of water and to re-inject water so that the fuel elements set down in the spent fuel pool remain sufficiently covered with water to ensure cooling and radiation shielding by means of the coolant.

5.3 (3) The safety-related acceptance targets for fuel element cooling are also fulfilled if the spent fuel pool is fully loaded (entire core unloaded).

The calculation of the water temperature is based on the respective most unfavourable conditions regarding residual heat and cooling conditions.

5.4 Level of defence 4

For events on level of defence 4, there exist no criteria beyond those according to Section 3.4.

6 Specific criteria for refuelling

6.1 Level of defence 1

N o t e: The following criteria for refuelling are restricted to the shuffling phase, including the loading and unloading of the fuel elements and core components, as well as to loading and functional tests.

6.1 (1) Protective measures are provided for the tasks involved in refuelling, especially with regard to shielding, building ventilation, and containment isolation.

6.1 (2) The coolant level in the reactor pressure vessel as well as the water level in the spent fuel pool are monitored and kept above the minimum level radiologically required for cooling.

6.1 (3) Measures and installations are provided that loose parts

a) cannot fall into the open reactor pressure vessel, and
b) are not flushed into the reactor pressure vessel during flooding or drainage of the reactor cavity.

Foreign matter or foreign bodies that might have fallen in or might have been entrained are recovered or it is demonstrated that leaving them in the system does not raise any safety concern.

6.1 (4) For nuclear power plants with pressurised water reactors,

a) it is ensured prior to the establishment of a connection between the reactor well and the spent fuel pool that the boric-acid concentration in the pool water and in the reactor well corresponds to at least the boric-acid concentration in the reactor and the spent fuel pool

that is specified for refuelling to ensure the required subcriticality; the required subcriticality is also maintained for the control rod free reactor core;
b) measures and installations are provided against impermissible entry of unborated water into the reactor coolant system;
c) the injection of boric acid with sufficient effectiveness for maintenance or re-establishment of the respective required subcriticality is possible at any time.

6.1 (5) During refuelling, neutron flux monitoring is ensured for the reactor core so that any approximation to the critical state is registered by measurements and corrective actions can be taken if required. In addition,

a) the boric-acid concentration in PWRs is monitored with sufficient time-based resolution at an appropriate location;
b) inspections are performed in BWRs during loading that ensure reliable control of the maintenance of the required subcriticality in the reactor core.

6.1 (6) In the case of the BWR, the control rods are inserted during refuelling, and their drives are rendered ineffective. The control rods attributed to the function and subcriticality tests are exempt for the duration of the inspections or tests.

6.1 (7) At least one residual-heat removal train is operational or on stand-by.

Coolant temperature is monitored.

6.1 (8) For the shuffling as well as for the loading and unloading of the fuel elements, a step-by-step schedule is prepared which covers each movement of fuel elements as well as control elements and control rods and also of all shuffling processes with further core components.

The performance of each individual step is recorded.

6.1 (9) For each step of the step-by-step schedule it is demonstrated that the required subcriticality is maintained, unless it is ensured that with this step, the required subcriticality is maintained.

6.1 (10) During refuelling, the fuel elements are only set down in the positions provided according to the step-by-step schedule.

6.1 (11) During development of the step-by-step schedule and its implementation, effective and reliable measures and installations are provided to prevent handling errors and any incorrect positioning of fuel elements. This is ensured, in particular, by
- careful planning and quality assurance for the shuffling and loading processes as well as quality-assuring measures during shuffling,
- high-quality and reliable refuelling machine pre-control devices,
- optimal ergonomic conditions regarding the handling devices,
- reliable communication between all those involved.

The step-by-step schedule considers that each fuel element handling process shall be carried out completely by one shift of personnel in one working operation.

6.1 (12) Examinations are performed to exclude that the reactor core is loaded with fuel elements that show impermissible bending, twisting or linear expansion.

6.1 (13) Prior to closing the reactor pressure vessel, the core load is checked for compliance with the planned load regarding the positioning and orientation of the fuel elements and core components. These checks are documented.

6.2 Level of defence 2

6.2 (1) The criteria according to subsection 6.1 (1), 6.1 (2), 6.1 (4c) and 6.1 (4) are fulfilled even in the case of events on level of defence 2.

6.3 Level of defence 3

For events on level of defence 3, there exist no criteria beyond those according to subsection 3.3 (1).

6.4 Level of defence 4

For events on level of defence 4, there exist no criteria beyond those according to subsection 3.4 (1).

7 Specific criteria for the loading and transport of fuel element transport and storage casks in nuclear power plants

7.1 Level of defence 1

7.1 (1) Only those fuel element transport and storage casks are used that have been specifically demonstrated to be appropriate for the respective nuclear power plant.

7.1 (2) It is ensured by appropriate measures and installations that
a) existing provisions regarding the admissible fuel element types, fuel element condition, burn-up values, source intensities, residual-heat levels and decay times are fulfilled upon loading;
b) the transport and storage cask is in orderly condition.

7.1 (3) Loading of the transport and storage cask takes place on the basis of a fuel-loading schedule and a description of the necessary working and testing steps prior to dispatch.

7.1 (4) The packing of the transport and storage cask is documented during loading. Before the cask is sealed, there is a full check of whether the cask has been loaded as specified.

7.1 (5) Fuel element transport and storage casks are only loaded in the position specially provided in the spent fuel pool or in a separate transport cask set-down pool.

7.1 (6) The load attaching points of the transport and storage casks and the handling devices used for loading and unloading the transport and storage casks meet the criteria according to Section 3.2.9 of the "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components" (Module 10).

7.1 (7) Contamination of the outer surface of the transport and storage cask is prevented/minimised by appropriate measures and installations. Installations are available to decontaminate the cask.

7.1 (8) Prior to dispatch from the plant, checks are carried out of the cask's leaktightness, the mechanical safety locks, the level of radiation, and any contamination with regard to the adherence to applicable limits.

7.1 (9) The transport and storage cask is secured against crashing and toppling over.

7.1 (10) Transport within the plant takes place via short and safe paths and without any unnecessary delays along a specified transport path. Transport across safety-relevant installations is avoided.

7.1 (11) The transport paths of the transport and storage casks are laid out such that the design conditions of the casks can be maintained.

7.2 Level of defence 2

7.2 (1) As far as the events on level of defence 2 mentioned in the list of events for the fuel pool in the "Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors" (Module 3) are relevant, these are controlled also under the conditions of "Transport or loading of transport and storage casks".

During loading of the transport and storage casks with fuel elements, the safety-related acceptance targets and acceptance criteria for fuel element storage and handling according to Table 3.1 of the "Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors" (Module 3) apply.

7.2 (2) Appropriate measures and installations are provided for the control of the consequences of events induced by anticipated operational occurrences. In addition to the events mentioned according to subsection 7.2 (1), the following anticipated operational occurrences are considered in particular:

– the failure to meet the leaktightness criterion,
– the failure of handling equipment during loading,
– the occurrence of leaks in fuel rods during dispatch,
– evacuation alert.

7.3 Level of defence 3

7.3 (1) As far as the events on level of defence 3 mentioned in the list of events for the fuel pool in the "Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors" (Module 3) are relevant, these are controlled also under the conditions of "Transport or loading of transport and storage casks".

During loading of the transport and storage casks with fuel elements, the safety-related acceptance targets and acceptance criteria for fuel element storage and fuel element handling according to Table 3.1 of the "Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors" (Module 3) apply.

7.3 (2) The stability of the transport and storage casks is given for all setdown positions, generally also in case of external events. Exceptions are limited to short-term, unavoidable set-down of the cask during the transport and handling process. The duration of set-down on these positions is limited to the time required.
N o t e: See also “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components" (Module 10), Section 2.2.4

7.4 Level of defence 4

7.4 (1) The stability of the transport and storage cask is given for all setdown positions, generally also for man-made hazard conditions, in case of aircraft crash only with regard to its consequential impacts. Exceptions are limited to short-term, unavoidable set-down of the cask during the transport and handling process. The duration of set-down on these positions is limited to the time required.
N o t e: See also “Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components" (Module 10), Section 2.2.4

L

MODULE 12
"Safety Criteria for Nuclear Power Plants:
Criteria for Electric Power Supply"

Contents

1 Scope

The following criteria apply to the electric power supply of installations in nuclear power plants executing functions with safety-related significance on levels of defence 1 to 4a or planned for accident management measures on levels of defence 4b and 4c.

2 Design

2 (1) The electric power supply of a nuclear power plant is designed such that on levels of defence 1 to 4a, the electric power supply of the consumers is ensured in compliance with their power supply conditions. It is designed such that its reliability will not be the determining factor of the unavailability of the systems to be supplied.

2 (2) The design of the installations for electric power supply and connected consumers is adjusted such that their stresses will not exceed the boundary conditions on which their design is based.

2 (3) Following power supply options are provided for the electric power supply of a nuclear power plant:

a) A unit generator which will sustain the electric power supply even in the event of a malfunction in the main grid or a loss of the main grid connection.
b) A main off-site power connection which will ensure the electric power supply in the event of unavailability of the unit generator.
c) A standby grid connection which will ensure the power supply in the event of unavailability of the unit generator and of the main grid; the standby grid connection is functionally separated and decoupled by protective circuits.
d) Emergency power supply facility generating units on the site of the power plant, ensuring the electric power supply of the emergency power consumers in the event of loss or unavailability of the supply options mentioned in a) to c).
e) An electric power supply independent of the supply options mentioned in a) to d) and ensuring at least the electric power supply of one residual-heat removal line, including the necessary instrumentation and control installations as well as the auxiliary and supply equipment.

2 (4) Installations for automatic adaptation of the unit generator in order to ensure sustained electric power supply in the event of disconnecting the unit from the grid are available.

2 (5) The main and standby off-site power connections are on principle connected to different voltage levels of the external supply grids in order to increase the reliability of the power supply of electric consumers by using power from different electric power stations as well as different separate off-site power grid switchyards and distribution facilities. If this cannot be fulfilled due to specific characteristics of the grid close to the power plant, at least the main and standby off-site power connections are connected to separate off-site grid switchyards and decoupled by protective circuits.

2 (6) The spatial arrangement of the standby grid connections and the auxiliary power system is implemented such that one single failure-initiating plant-internal event or one single failure-initiating event within the electric power supply of the nuclear power plant or in the area of the grid connections will not result in a long-term failure of all grid supply possibilities. Such a failure-initiating event, like a random failure including consequential mechanical damage, an internal event or an external event, except for earthquake, will not lead to a long-term failure of all power supply possibilities according to subsection 2 (3) b, c and e.

2 (7) At least one connection to the grid or a power plant in the vicinity of the nuclear power plant is installed as an underground cable.

2 (8) Main and standby grid connections are designed in such a manner that each of them is able on its own to ensure the electric power supply of the installations that execute the required functions on levels of defence 1 to 4a.

Main and standby grid connections as well as the energy supply possibilities according to subsection 2 (3) are dimensioned in such a manner that each of them on its own is able to provide for electric power supply of the installations for accident management measures (levels of defence 4b and 4c).

2 (9) The switch-over from the main off-site power connection to the standby grid connection takes place automatically if the electric supply conditions via the main grid connection can no longer be ensured and standby grid is available. The actuation set points and the time delays of this automatic switch-over mechanism are adjusted with those of the automatic starting mechanisms of the emergency power generators in such a way that no unnecessary connections to the emergency power facilities will occur by electrical transients.

2 (10) For emergency power supply, redundantly designed emergency power supply facilities are provided. The redundants of the emergency power supply facilities are independent of each other. The degree of redundancy of the emergency power supply facilities corresponds at least to the redundancy degree of the process systems to be supplied. The degree of redundancy fulfils the criteria for the control of single failures according to the "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components" (Module 10), Section 1.1.

2 (11) The emergency power system is on principle built by redundants, segregated redundants of the emergency power supply facilities which guarantee functional independence between the redundants by their design. If thus the degree of reliability required by the system to be supplied is not achieved, emergency power consumers may be supplied by more than one redundant of an emergency power supply facility, meeting following conditions:

a) the reliability of the emergency power system is not unduly reduced, and
b) connections are implemented such that none of possible failures to be taken into account can cause the failure of more than one redundant of an emergency power supply facility.

2 (12) Failure-initiating events within the emergency power system do not lead to a loss of necessary power supply of the equipment executing functions on levels of defence 3 to 4a.

2 (13) The redundants of emergency power supply facilities are physically separated or protected from each other such that any failure-initiating events in the emergency power supply facility will not lead to a loss of several redundants of an emergency power supply facility.

2 (14) The auxiliary systems and the auxiliary media supply of the emergency power supply facility are designed such that they correspond at least to the degree of redundancy of the emergency power system and will not determine the reliability of the emergency power supply system.

2 (15) The startup and connection of the emergency power generators runs automatically on demand, so that no manual actions are required within 30 min. Manual startup and connection of the emergency power generators to the bus bars is possible at any time.

2 (16) The conditions for shutting down the operation of the emergency power supply facility generating units are given if the supply via the main grid connection or the standby grid connection or another supply connection is reliably available for the consumers of the emergency power supply facilities. The switch back to the available grid connection is initiated manually.

2 (17) The installations of the emergency power supply system are designed such that complete tests of the safety-relevant features are possible.

2 (18) Simultaneous testing of redundants of an emergency power supply facility is reliably prevented.

2 (19) The emergency power supply facilities are designed and protected such that in case of external or internal events, not all redundants of the emergency power supply facilities will lose their functional condition simultaneously. The redundants of the emergency power supply

facilities that have not lost their operability are sufficiently effective to control events on levels of defence 3 and 4a.

2 (20) If in case of external events, a simultaneous loss of all grid connections cannot be excluded, measures and installations are provided that after 3 days at the latest, supply can be restored via a grid connection provided according to subsection 2 (3) b or c, or can be established via a supply possibility according to subsection 2 (3) e.

2 (21) The protection against external and internal electromagnetic impacts is designed such that the electrical installations of the energy supply which supply the installations with functions on levels of defence 1 to 4 are not unduly impaired.

2 (22) The following measures and installations are provided to control a loss of the electric power supply of the nuclear power plant, including the emergency power generators:

a) Provision of energy storage systems with sufficient capacity in order to be able to execute the necessary functions until restoration of the electric power supply, but at least for 2 hours.
b) an additional possibility of supply to the main and standby off-site power connections by which the electric power supply of the necessary functions can be established before depletion of the energy storage devices.

3 Quality assurance and tests

3 (1) The required quality of the electrical installations of the energy supply is ensured by quality assurance measures.

The suitability of the electrotechnical components for the use in nuclear power plants is demonstrated by type tests and proven performance. For additionally required safety-related features, e.g. design for loads due to external events and against design-basis accidents (resistance against design-basis accidents) not covered by proven performance and type tests, additional suitability demonstrations are performed.

3 (2) The installations of the emergency power system are subjected to regular-in-service inspections. If necessary for reasons of reliability, tests are also carried out during power operation. All tests are documented.

3 (3) The installations in the emergency power system are monitored for operability and their operating condition by means of measurements and signals.

M

Terms and Definitions
"Safety Criteria for Nuclear Power Plants: Terms and Definitions"

A

Ability of mechanical shutdown
A condition of the reactor core in which its shutdown by means of the control elements (PWR) or control rods (BWR) can be ensured on the basis of the prevailing geometrical configuration of the reactor core.

Abnormal operation
Operational processes that develop in the event of malfunctions of installations or human errors (disturbed operating condition) whose occurrence is frequently to be expected over the service life of the plant concerned from operating experience and for which there are no safety-related reasons against a continuation of operation or the activity (level of defence 2).
Synonym: Anticipated operational incident.

Acceptance criterion
A criterion the fulfilment of which has to be demonstrated in the course of the safety demonstration.

Acceptance target
Safety-related objective of the safety demonstration which is reached by fulfilment of acceptance criteria.

Accident
Event or event sequence which is not expected to occur during the service life of the plant, however the plant is designed such that the design principles, acceptance targets and acceptance criteria of level of defence 3 are fulfilled, and in case of its occurrence operation of the plant or the action can not be continued due to safety reasons.
Synonym: design basis accident

Accident analysis
Analysis of the sequence of an event on level of defence 3 (accident).

Accident instrumentation
Installation which registers, displays and records information on the condition of the plant before, during and after a design basis accident or an event which may lead to an increased release of radioactive materials.

Accident involving severe core damage
Event sequence with severe core damage

Accident management
Measures and installations on levels of defence 4b and 4c.

Accident management guideline
Generic approach that can be applied if for event sequences or plant conditions no accident management measures have been planned or these accident management measures are not effective as planned.

Accident management measure
Special measure planned and / or installation of accident management in the preventive and mitigative area.

Accident management procedure
Written instruction for the necessary step-by-step actions to execute an accident management measure.

Accident management strategy
Written instruction for the employment of accident management measures and accident management guidelines.

Activities and processes, safety-relevant

All activities and processes that may have an influence on the safety of the nuclear power plant.

Ageing
Time-dependent and use-bound changes of function-related features and characteristics
- of the technical installations (components, structures, systems, including electrical systems and instrumentation and control),
- of the specification and other reference documents,
- of the plant concept and technological procedures,
- of administrative regulations, as well as
- of the operating personnel.

Ageing management
The entirety of all measures and installations to be provided by the licensee to control the ageing phenomena that are relevant with regard to the safety of a nuclear power plant.

Alarm system
Instrumentation and control installation signalling the necessity of a measure by optical or acoustic means.

Anticipated operational occurrence
Event or event sequence which is expected to occur frequently during the service life of the plant, and upon whose occurrence the operation of the plant or the activity can be continued, and for which the plant is designed or for which, with regard to an activity, measures and installations are provided as a precaution (level of defence 2). Synonyms: abnormal operation, disturbed operating condition.

Application profile of the software
The way in which the software is used, including the time-dependent criteria, the data to be processed, the parameters used and the user interferences to be performed.

Auxiliary and supply systems
Systems that may be required for the functions of other systems or components.

Auxiliary power supply
The electricity supply of the consumers connected to the auxiliary power system and of the systems supplying the emergency power system from the unit transformer, the main or standby grid, or from other external grids.

Auxiliary power system
Entirety of all plant components that serve for the electricity supply of the consumers connected to them and for feeding into the emergency power system.

B
Basic safety
Basic safety means that if the corresponding principles upon design, construction, manufacture and testing are adhered to, no far-reaching failure of a component due to manufacturing-related deficiencies is postulated.

Boiling condition, critical
Boiling condition when film boiling or when dryout of the heating surface starts.

Boron dilution, heterogeneous
Injection of low-borated coolant with consequential significant boron concentration differences in the primary circuit.

Boron dilution, homogeneous
Injection of low-borated coolant without consequential significant boron concentration differences in the primary circuit.

Building, structure

Synonym for plant structure.

C

Cladding damage
Gas leakiness of the fuel rod cladding.

Company
The organisation of the licensee of the nuclear power plant. The company comprises the personnel, equipment and rights, including the plant itself and the organisation, necessary to operate the nuclear power plant. For the purpose of these “Safety Criteria for Nuclear Power Plants”, other companies with a share in the company, dominant companies or companies otherwise associated with the licensee or parts of such companies that are referred to as part of the company in the licensee's documentation of the management system as far as they perform processes or activities or have tasks and responsibilities or authorisations that may have an influence on the safety of the nuclear power plant shall also be considered as part of the company.

Component
Part of a system defined separately according to structural or functional aspects.

Component part
Part of an installation or the smallest part of a subassembly manufactured from product forms.

Component, passive
A component is passive if there will be no change in its positioning in case of challenge (e.g. pipes, vessels, heat exchangers). Self-acting components (functioning without external power or control) shall be considered as passive if the position of the component under consideration (e.g. safety valve or check valve) is not changed in the course of fulfilling its intended function.

Conservative
The way of proceeding in safety assessments under consideration of the most unfavourable values from a safety point of view under the given circumstances

Containment penetrations
Designs that allow the pressure-proof and technically leak-tight penetration of lines (e.g. medium-containing pipes, cables) through the containment.

Containment system
System consisting of containment and surrounding building as well as the auxiliary systems for retention and filtering of potential leakages from the containment.

Control room
The central location from which the operation of a nuclear power plant unit is monitored and controlled. Parts of the main control room are the actual control room and the adjoining rooms (control room annex).

Control station, local
Installation outside the control room from which systems can be monitored and controlled.

Coolability
Condition of the reactor core in case of which the removal of the heat produced and stored can be ensured.

Cooling water
Water which during normal operation is not contaminated with radioactive materials and which has the function of heat transfer to the main heat sink (e.g. receiving water, cooling tower).

Core component
Component part or component of which the reactor core is composed, comprising, in particular: fuel elements, control elements or rods, flow restrictor assemblies, poisoning and dummy

elements, fuel channels and channel fasteners, neutron sources, neutron-absorbing devices of the fuel elements and detector assemblies.

Core damage, severe
Condition of the reactor core with which coolability and / or permanent subcriticality is no longer given.

D

Decay heat
The thermal power produced after reactor shutdown by radioactive decay or fission (see also residual heat).

Design
The process and result of a concept development including the detailed planning of a plant or plant components on the basis of the provisions regarding the impacts and boundary conditions to be taken into account and the requirements for safety demonstration.

Design basis accident
see: Accident

Design criterion
Specification of provisions for a design resulting from the conventional rules and regulations and from the safety requirements specific to nuclear power plants.

Design limit
Acceptance criterion for a parameter considered in the design; if this criterion is complied with, a failure of the plant component concerned need not be postulated.

Design, inherently safe
Design on the basis of those principles of the laws of nature which by themselves have a safety-directed effect.

Disaster control measure
Precaution for the protection of the population for the case that in the event of a beyond-design-basis plant condition significant releases of radioactive materials into the environment occurred or must be feared (level of defence 5).

Discharge of radioactive materials
Discharge of radioactive materials in either liquid or gaseous form or bound to suspended matter from the plant via paths specially provided for this purpose.

Dissimilar instrumentation and control installations
Instrumentation and control installations consisting of different hardware and software (if software is used), characterised by the deployment of different development tools, development teams, production processes, tests and maintenance strategies.
Note: Hard-wired instrumentation and control installations performing instrumentation and control functions without the use of software are on principle dissimilar to the software-based instrumentation and control installations.
The instrumentation and control installations that serve the manual actuation of safety functions are dissimilar to the automatic instrumentation and control installations if they are not affected by the postulated systematic failure.

Diversity
Availability of two or more operable installations to fulfil the intended function, having different physical or technical designs.

E

Emergency control room
Installation outside the control room from which in case of failure of the control room, the reactor can be made subcritical, subcriticality can be maintained and heat removal from the core after its shutdown can be monitored and controlled.

Emergency power consumer
An electrical consumer which is supplied from an emergency power supply facility.

Emergency power generator
Installation that supplies the electrical energy in case of loss of the auxiliary power supply.

Emergency power supply
Supply to the emergency power consumers from emergency power generators.

Emergency power supply facility
The combination of a specific emergency power generator with all component parts required for the supply to the associated consumers.

Emergency power supply, uninterrupted
Emergency power supply where after failure of the supply from the auxiliary power supply system or from grid connections, supply from an emergency power generator (or an electrical energy store) starts without interruption.

Emergency power system
Entirety of the emergency power supply facilities differing in type of generation and task.

Emergency system
Measure and / or installation required for the control of a case of a man-made hazard.

Error
(1) Deviation of the specification from the actual requirements (specification error).
(2) Deviation of the actual design of a plant component from the constructive and manufacturing-related design of the plant component required for the compliance with the specification.
(3) Deviation between the value calculated, observed or measured and the true, specified or theoretically correct value.

Event
Event that potentially or actually impairs the safety of a plant.

Event analysis
Analysis element of the deterministic safety analysis. Method of safety demonstration by which it is demonstrated that sufficiently effective measures and installations are available for the control of events.

Event, representative
Event whose analysis allows an adequate, generically covering safety demonstration.

External event
Impacts caused by the ambient conditions, natural events or external man-made influences from outside the plant site.

Failure
Non- or malfunction in case of challenge of active systems or loss of integrity or operability of passive systems.

Failure of an instrumentation and control installation, active
Malfunction of an instrumentation and control installation leading to spontaneous performance of an instrumentation and control function without fulfilling the criteria specified for the performance.

Failure of an instrumentation and control installation, passive
Malfunction of an instrumentation and control installation by which an instrumentation and control function is not performed when challenged although the criteria specified for the performance are fulfilled.

Failure probability
Probability of the failure of the plant component concerned, derived on the basis of experiments, in dependence of the respective parameter considered.

Failure, loss
Loss of the ability of an installation to fulfil the required function.

Feedback, thermal
Loop which is generated if the internal pressure of the fuel rod leads to lifting of the fuel rod cladding to such a degree that there will be an impairment of the fission heat transfer, an increase of the fuel temperature, increased release of fission gas and, finally, further increase of the internal pressure.

Feedwater
Water for secondary-side supply to the steam generators in PWR plants or for operational feed of the reactor pressure vessel in BWR plants.

Film boiling
Boiling process during which there is a stable steam film between the cladding tube and the cooling liquid.

Forced reactions under normal operational loads
Reactions of plant structures to operational impacts; e.g. forces and moments from temperature, creep, shrinkage and support displacement.

Fuel rod damage
Synonym for cladding damage.

G
Grid connection
Connection between power plant and grid though which the electrical energy can be transmitted.

H
Hazard, man-made
Event sequence due to a very rare human-induced external event or due to the postulated complete unavailability of the control room.

Human error
Non-compliance with a requirement during a personnel action.

I
Impact
Forces or media with physical, chemical or biological effects or a combination of them acting on installations.

Incorporation
Intake of radioactive materials into the human body.

In-service inspection
Inspection performed at specified intervals.

Inspection
Measure for the identification and assessment of the actual condition.

Installation
Synonym for plant component.

Installation, safety-relevant

Installation
- whose failure leads to uncontrollable event sequences, or
- that is required for effective and reliable control of design-basis accidents, including the auxiliary and supply systems required for it, or
- that is required for effective and reliable prevention of events, including the auxiliary and supply systems required for it, or
- that serves the compliance with and monitoring of specified radiological values, in particular by maintenance of the required effectiveness of barriers and retention functions, or
- that serves the performance of tasks with safety-related significance which is not assigned to the above-mentioned conditions.

Instrumentation and control
The entirety of the instrumentation and control installations for the performance of instrumentation and control functions. Instrumentation and control installations comprise automatic installations as well as the installations for process control by an operator.

Instrumentation and control function
Function for measuring, managing, controlling, monitoring, recording and protecting a process or an installation (German abbreviation: LEFU)

Instrumentation and control installation
Installation for the execution of instrumentation and control functions.

Integrity
Condition of a component or barrier with which the safety-related criteria regarding strength, resistance to fracture and tightness defined for them are fulfilled.

Interlock
Provision by means of which functions of installations which are impermissible under specified operating or design-basis-accident conditions are blocked by instrumentation and control or process-related mechanisms.

Internal event
Impacts resulting from events within the plant site (e.g. fire, plant-internal flooding).

Internal flooding
Floodings in buildings or at the plant site not being due to an external event.

L

Leak
Continuous or discontinuous outflow of media from the respective enclosures (e.g. vessels, piping systems, fuel pool) with an outflow rate to such a high level that safety installations are challenged.

Leak, large
Leak with an outflow surface > 0.1 A (A: cross-sectional area of the main coolant line).

Leak, medium
Leak with an outflow surface ≤ 0.1 A (A: cross-sectional area of the main coolant line) and where, for PWRs, primary-side heat removal through the leak outflow is sufficient such that secondary-side heat removal is not necessary for the control of design-basis accidents.

Leak, small
Leak with an outflow surface ≤ 0.1 A (A: cross-sectional area of the main coolant line) and where, for PWRs, secondary-side heat removal is necessary for the control of design-basis accidents.

Leakage

Continuous or discontinuous outflow of media from the respective enclosures (e.g. vessels, piping systems, fuel pool) with an outflow rate that remains at such a low level that safety installation are not challenged.

Level of defence
Category of plant conditions with defined boundary conditions of similar type:
Level of defence 1: normal operation
Level of defence 2: abnormal operation
Level of defence 3: design-basis accident
Level of defence 4: very rare events (level of defence 4a),
events with multiple failure of safety installations (level of defence 4b),
accident involving severe core damage (level of defence 4c).

Licensee
The natural or legal person(s) or private company(ies) with partial legal capacity authorised to operate the nuclear power plant by one or more licences.
N o t e: For legal persons and private companies, distinction is to be drawn between
- the responsibility of the respective corporation as licensee of the nuclear power plant,
- the attending to this responsibility by the corporate management, i.e. the board members, general managers or another body of this corporation which is authorised to represent by law, statutes or contract, as well as
- the tasks, responsibilities and authorisations of other persons and organisational units of the company that are derived from the licensee's responsibility.

Limitation system
Instrumentation and control installation with one of the following functions:
- Operational limitation: Limiting process variables to set values in order to increase the availability of the plant.
- Protective limitation: Actuation of those protective actions that return monitored safety variables to values at which a continuation of specified normal operation is permissible.
- Limiting process variables: Limitation of process variable values to maintain initial conditions for design-basis accidents to be considered.

Load-carrying capacity
Maximum permissible loading by a static load.

Loading level
Common classification of loads in technical standards for pressure-retaining components and plant structures. Here, impacts ("load cases") to be postulated a n d / o r specified are classified according to their effects (loadings) and requirements for safety demonstration in connection with the assessment procedure (stress categorisation). The relevant KTA safety standards (KTA 3201.2, 3211.2, 3401.2) demand plant- and system-specific classification right down to the component level.

Local dose
Equivalent dose, measured at a given location by means of the quantity to be measured as specified in Appendix VI, Part A of the Radiation Protection Ordinance (StrlSchV).

Local dose rate
The local dose generated in a given time interval, divided by the length of that time interval.

Loss-of-coolant accident
Event with loss of reactor coolant from the reactor coolant pressure boundary such that the safety system is challenged.

Low-power and shutdown operation
The operating phases that do not serve a targeted nuclear heat production (operating phases B to F).

M
Main grid
The grid to which the electrical energy produced by the nuclear power plant unit is discharged or from which electrical energy is supplied.

Main grid connection
A grid connection via which the electrical energy produced by the nuclear power plant unit is discharged to the grid or via which electrical energy can be supplied.

Maintenance
The entirety of the measures for maintenance and restoration of the specified condition as well as for the identification and assessment of the actual condition (including in-service inspection). Maintenance is subdivided into inspection, servicing and repair.

Management cycle, closed
Performance of activities in processes, using the “plan-do-check-act“ cycle.

Management system
Organisational system which, in particular, defines the way in which safety management is performed and specified and comprises the related organisational structures, regulations and aids for planning, performance, review and continuous improvement of all activities and processes. The management system integrates all requirements for the company and the safety-relevant activities and processes resulting from the different aspects, such as safety, environment, quality, finances, etc..

Measure
Action, instruction or organisational activity or organisational process.
N o t e: If no action, instruction or organisational activity is referred to, the measure is further specified, e.g.: accident management measure, disaster control measure, etc.

Multiple failure of safety installations
Event sequence with failures of safety installations such that sufficient effectiveness of safety functions for the control of design-basis accidents is no longer given.

N
Normal operation
The operating conditions and processes during functional condition of the installations (undisturbed condition), including in-service inspections and maintenance processes (level of defence 1).

Normal operation, specified
The mode of operation for which a plant has been intended and designed and for which it is suitable according to its technical purpose, comprising the operating conditions and processes
- under functional conditions of the installations (undisturbed operating condition, normal operation, level of defence 1),
- of abnormal operation (disturbed operating condition, anticipated operational occurrence, level of defence 2), as well as
- during maintenance processes (inspection, servicing, repair).

O
Operability
Ability of an installation to fulfil the tasks specified by the corresponding mechanical, electrical or another function.

Operating phase
Operating conditions of normal operation for which specific criteria for availability of system and monitoring functions as well as for process-related conditions are defined.
Note: The following operating phases are defined and used in the “Safety Criteria for Nuclear Power Plants”:
Operating phase A: power operation
Operating phase B: startup and shutdown
Operating phase C: residual-heat removal operation, RCS closed
Operating phase D: residual-heat removal operation, RCS open, not flooded
Operating phase E: residual-heat removal operation, reactor flooded
Operating phase F: Core unloaded, spent fuel pool lock closed

Operation management
The entirety of all processes and activities that are necessary for the operation of the plant.

Operation monitoring
Controlled recording of operating parameters, including a comparison with specified values.
N o t e: Monitoring is performed e.g. by continuous measurement, discontinuous analysis of samples or calculation of values by correlation of measured values.

P

Personal dose
Equivalent dose, measured by means of the quantity to be measured as specified in Appendix VI, Part A of the Radiation Protection Ordinance (StrlSchV) at a part of the body surface which is representative for radiation exposure.

Physical separation
Arrangement of redundant subsystems with spatial distance or separated by appropriate plant structures.

Plant component
Any structural, mechanical, process-based, electrical or other technical part of a plant. Synonyms are: installation, system.

Plant condition
Technical condition of the plant, e.g. characterised by the plant's power output and by temperature, pressure and coolant level parameters of the reactor coolant system.

Plant condition, beyond-design-basis
Plant condition after an event with failures of safety installations such that effectiveness sufficient for the control of a design-basis accident is no longer given (see also Multiple failures of safety installations).

Plant condition, controlled
Plant condition after occurrence of an event characterised in that the protection goals are complied with and the relevant safety variables have reached stationary values.

Plant condition, safe
Plant condition after occurrence of a design-basis accident characterised in that a controlled plant condition is given and the safety installations required for maintenance of a controlled plant condition are available with resistance to a single failure.

Plant management level
The plant manager and the persons one level lower in the hierarchy.

Plant manager
Staff member who bears the responsibility for the safe operation of the entire plant, in particular for the adherence to the stipulations of the nuclear legislation and the nuclear licences as well as for the co-operation of all departments and who is authorised to give instructions to the heads of departments or sections.

Plant operating procedures
All written documents that are needed for the operation of the plant. They include, in particular, the operating manual, emergency operating procedures, testing manual, and procedural and working instructions.

Plant structure
Part of the plant assembled from building products (building materials and component parts) and connected with the ground.

Power density oscillation, (global, regional)
Thermal-hydraulic neutron-physically coupled oscillations of the neutron flux:
1. global: the neutron flux oscillates in phase over the entire core (also referred to as in-phase or core-wide oscillation);

2. regional: one half of the core oscillates out of phase to the other (also referred to as out-of-phase or local oscillation).

Power operation
The operating phase of a nuclear power plant in which nuclear heat is produced in a targeted manner (operating phase A).

Preventive measure
Measure(s) and / or installation(s) in case of whose existence occurrence of an event has been demonstrated to be so unlikely that it does not have to be postulated.

Primary circuit
System area which comprises the reactor coolant pressure boundary in PWR plants.

Primary coolant
Water which serves the direct cooling of the reactor core in PWR plants.

Process variable
A chemical or physical quantity of the process that can be measured directly.

Process, organisational
Set of interrelated or interacting activities that transforms inputs into results.

Protection goal
Fundamental safety function that comprises different subordinate safety functions to be ensured for fulfilment of the respective acceptance targets and acceptance criteria.
The protection goals are:
a) reactivity control,
b) fuel cooling,
c) confinement of the radioactive materials.

Protective action
The actuation or operation of active safety installations that are needed for the control of event sequences.

Protective limitation
See limitation system.

Q
Qualification of persons
The existence of knowledge, abilities (physical and psychical) and skills (learnt or trained behaviour patterns) as well as attitudes to be able to behave according to the demands.

R
Reactor coolant
Water which serves the direct cooling of the reactor core in PWR and BWR plants.

Reactor coolant pressure boundary
Entirety of all pressure-retaining boundaries of the components of the pressure zone of the reactor pressure vessel up to and including the first isolating valve; for piping of the pressure zone of the reactor pressure vessel penetrating the containment, up to the first isolating valve outside the containment.

Reactor coolant system
System which comprises the reactor coolant pressure boundary in PWR and BWR plants.

Reactor protection system
The part of the safety system which monitors and processes the process variables relevant for safety and initiates protective actions for the prevention of undue impacts and registration of

design-basis accidents (level of defence 3) in order to keep the condition of the reactor plant within safe limits.
As part of the safety system, the reactor protection system comprises all installations for the recording of measured values, of signal conditioning, of the logic level and parts of the control assigned to the individual drives for initiating protective actions as well as the functional group control.

Redundancy
Existence of more operable installations than required for the fulfilment of the intended function.

Redundancy-wide event
Internal event or external event with the potential to cause system- and redundancy-wide failures.

Redundant
Installation which on par with other installations fulfils their functions and, if required, can completely replace one of the other installations or can be replaced by it.

Refuelling
The entirety of all operational activities required to shuffle irradiated fuel elements or replace those that are defective and are to be removed from the core.

Release category
Release categories comprise sequences from the accident analyses with similar radionuclide releases under consideration of further characteristics of the release (e.g. nuclide properties, such as, in particular, radiotoxicity and volatility, nuclide composition, time of release after occurrence of the event, duration, level, energy content).

Release of radioactive materials
Inadvertent escape of radioactive materials from the enclosures provided into the plant or into the environment due to events on level of defence 3 or 4.

Residual heat
Total of the heat produced by the decay heat and the heat stored in the coolant and in components or plant structures.

Residual- heat removal system
System for the removal of residual heat.

Residual-heat removal operation
Removal of residual heat with the residual-heat removal system.

Retention efficiency
The mass ratio between the amount of a material separated in a separation process and its original total amount.

Retention function
Measure and / or installation for the retention of radioactive materials, e.g. by filtering, water coverage, guided flow by maintenance of subatmospheric pressure, delay lines, vessels and other enclosures.

S

Safety analysis, deterministic
Analysis of the safety-related condition of a plant or a plant component for verifying the fulfilment of the deterministic safety criteria, consisting of a system assessment and a condition or event analysis.

Safety analysis, probabilistic (PSA)
Analysis of the safety-related condition of a plant by determination of the frequency of hazard or core damage states or the frequency of the release of radioactive materials.

Safety culture
Safety culture is determined by a safety-oriented attitude, responsibility and conduct of all staff required for ensuring the safety of the plant. For this purpose, safety culture comprises the assembly of characteristics and attitudes in a company and of individuals which establishes that, as an overriding priority, nuclear safety receives the attention required by their significance. Safety culture concerns both the organisation and the individual.

Safety demonstration
Verifiable information and data which demonstrate the fulfilment of requirements. A demonstration can be performed, among others, by analyses, experiments and measurements, test reports, certificates or by combining these forms of demonstrations.

Safety distance
Difference between a parameter and a value in case of which the loss of the required characteristic can no longer be excluded.

Safety function
Functional combination of measures and installations for the fulfilment of safety-related tasks.

Safety installation, active
Installation of the safety system performing protective actions.

Safety installation
Installation of the safety system serving the control of design-basis accidents.

Safety management
Entirety of all activities relating to the planning, organisation, management and supervision of individuals and work activities for assurance and continuous enhancement of safety as well as for the promotion of a highly developed safety culture. Safety management is not limited to certain organisational units.

Safety margin
Additional margin to protect against uncertainties.

Safety policy
Overall intentions and direction of an organisation with regard to safety.

Safety system
The entirety of all installations that have the task to protect the plant against undue impacts and, in case of design-basis accidents, to keep their effects on the operating personnel, the plant and the environment within specified limits.

Safety variable
Safety-relevant operating parameter and / or safety-relevant process variable.

Segregation
Separation of system parts to avoid mutual disturbance.

Senior management
Individuals or groups of individuals that manage and control a company at top level. For legal persons or private companies with partial legal capacity, these are the board members, general managers or another body of this corporation which is authorised to represent by law, statutes or contract. A distinction is to be drawn between the senior management and all other persons in charge of managerial tasks and the execution level (all persons executing safety-relevant activities).

Shutdown (of the plant)
Controlled transfer of the plant from operating phase A or B to operating phase C.

Shutdown reactivity
The reactivity of the reactor transferred to a subcritical condition by means of the shutdown achieved by the installations provided for this purpose.

Shutdown system
An installation that is able to transfer the reactor to a subcritical condition and maintain it in this condition.

Single failure
A failure that is additionally assumed to occur in installations in the challenge case considered independent of the initiating event, but which does not occur as a consequence of the challenge case and is not known before the challenge case itself has occurred. The single failure also includes the consequential failures resulting from a postulated single failure.

A single failure has occurred if a system part of the installation does not fulfil its function upon challenge. An incorrect operation that is possible under operating conditions and which results in a malfunction of the installation is equated with a single failure.

A single failure in a passive installation means the failure of this installation.

Single failure concept
Concept of combining failure assumptions due to an active or passive single failure and maintenance processes.

Software failure
Non-fulfilment of functions of the software.

Spread of radioactive materials
Inadvertent spread of open radioactive materials.

Support stability
Safety against undue alteration of position and place of a plant component (e.g. overturning, dropping, inadmissible slipping).

Standby grid
Grid from which the nuclear power plant unit can be supplied with electrical energy via the standby grid connection.

Standby grid connection
Grid connection via which at least the electrical energy for shutdown of the nuclear power plant can be supplied under maintenance of the main heat sink.

Startup
The controlled transfer of the plant to operating phase A (power operation).

Subassembly
Part of a component that consists of at least two component parts.

Subsystem
Part of a multiply structured (of similar type) system that partially or completely fulfils the function of the system.

Suitability for use
Ability of a plant structure to enable use as planned under the impacts considered in the planning.

Supply system
System for the provision of, e.g., electrical energy, unborated water, auxiliary steam, cooling water, heat, cold, compression air or other technical gases or lubricants.

Surface contamination
Decontamination of a surface with radioactive materials comprising activity that is non-fixed, fixed and has penetrated through the surface.

Surface contamination, non-fixed
Decontamination of a surface with radioactive materials for which spread of the radioactive materials cannot be excluded.

System
Synonym for plant component.

System assessment
Analysis element of the deterministic safety analysis for verifying the fulfilment of quality criteria.

System part
Synonym for component.

Systematic failure
Failure due to the same cause.

T
Test
Measure for determining whether the actual condition corresponds to the specified condition.

Transient
Disequilibrium between power release and power removal, developing in a dynamic way.

V
Validation
Review of the validity and accuracy of the obtainable results of calculations by means of examples using exact analytical solutions or by means of experiments or other calculation methods which have already been verified.

Verification
Confirmation by provision of objective proof that specified criteria are fulfilled.