Safety Requirements for Nuclear Power Plants

03 March 2015

Note:
This is a translation of the document entitled:
"Sicherheitsanforderungen an Kernkraftwerke".

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

Apart from this Main Part, the "Safety Requirements for Nuclear Power Plants" include five Annexes.

Contents

Scope of application

The "Safety Requirements for Nuclear Power Plants" apply to facilities for the fission of nuclear fuels for the commercial generation of electricity (nuclear power plants). They contain fundamental and general safety-related requirements within the framework of the non-mandatory safety standards and rules that serve for substantiating the precaution that pursuant to § 7 para. 2 no. 3 of the Atomic Energy Act (AtG) is necessary according to the state of the art in science and technology to prevent any damage caused by the construction and operation of the plant as well as the requirements of § 7d AtG. Regarding the nuclear power plants operated in Germany, this concerns modification licenses. Here, the decisions of the Supreme Court on the scope of regulatory examination in modification licensing procedures shall be considered.

The "Safety Requirements for Nuclear Power Plants" shall furthermore be applied in safety-related assessments within the framework of §§ 17, 19 AtG; however, their publication gives no reason for a special safety review. What has been determined in the respective licenses continues to be valid as far as this is not called into question by recent findings and hence has to be re-assessed. Any intervention in valid licenses is only possible under the conditions laid down in § 17 AtG.

The "Safety Requirements for Nuclear Power Plants" include the “Safety Criteria and Guidelines for Nuclear Power Plants” within the meaning of § 49 para. 1 sentence 3 of the Radiation Protection Ordinance (StrlSchV) in updated form.

Requirements for physical protection are not included.

As far as necessary from a safety-related point of view, the "Safety Requirements for Nuclear Power Plants" shall also apply to nuclear power plants that pursuant to § 7 para. 1a AtG have had their power operating licenses revoked or which due to a decision taken by the licensee are in their post-operational phase.

The technical terms used are defined in Annex 1 as far as necessary. Annexes 2, 3, 4 and 5 underpin or supplement the Safety Requirements. In Annex 2, requirements regarding postulated events are substantiated, while those regarding the protection against internal and external hazards as well as very rare human-induced external hazards are specified in Annex 3. In Annex 4, the fundamental principles for the application of the single-failure criterion and for maintenance are substantiated, while in Annex 5 the requirements for safety demonstration and documentation are specified.

0 Fundamental principles

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

The licensee is responsible to assure plant safety. He shall give 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 organizational factors (man-technology-organisation). The inter-connection of these factors with the aim to act in a safety-oriented manner is also the basis for a highly developed safety culture. It is the licensee's task to maintain this safety culture and to enhance it continuously.

1 Organisational requirements

1 (1) Responsibility of the company management

It is the responsibility of the company management to ensure the safe operation of its plant.

Within the framework of this responsibility, the company management shall fulfil in particular the following requirements:

1. the development, introduction and continual improvement of an integrated, process-oriented management system (IMS);
2. the definition and implementation of the company policy and business objectives in which the company commits itself to a high level of safety and to a strengthening of the safety culture; here, it has an exemplary function;
3. guaranteeing that the company policy and the business objectives are communicated and implemented by the plant management;
4. the preparation of principles regarding the organisational structure and the procedural organisation;
5. the provision of the necessary resources (organisational, administrative, technical) for the company and the plant. For this purpose, adequate financial and human resources shall be permanently provided and kept ready by the licensee to fulfil his duties regarding safety. The development of the personnel to maintain core competence and broaden competences shall be guaranteed and periodically reviewed;
6. the nomination of the plant manager responsible for the safe operation of the plant and of the officials demanded by the regulatory requirements.

This responsibility cannot be delegated or outsourced. The company management shall set an example of safety-directed acting and actively support the latter.

The company management shall ensure that the internal and external feedback of experience, changes in the state of the art in science and technology and of proven international safety practices including the associated information arranged by authorities is systematically registered, evaluated and documented in a process of the management system.

1 (2) Responsibility of the plant management

Within the framework of its responsibility, the plant management shall fulfil in particular the following requirements:

1. Drawing-up and implementation of plant policy and targets in line with the company policy and business objectives.
2. Guaranteeing the safe operation of the plant.
3. Adherence to the legal, regulatory and safety-related requirements.
4. Development and introduction of the IMS in the plant. This shall involve the entire personnel.
5. Implementation and continual improvement of the IMS including its influence on safety.

6. Determination and implementation of the organisational structure and the procedural organisation within the plant.

7. Guaranteeing the necessary competences and training of the personnel. Here, the plant management shall be mindful that training considers not only technical aspects but also methodical competence and that attitudes towards safety-directed acting are promoted.

8. Assurance of the execution of safety-relevant jobs by personnel that demonstrably has the requisite qualification.

9. Registration, evaluation, utilisation and communication of internal and external experiences. Here, the plant management shall be mindful that regarding the internal feedback of experience, information about near- miss events shall be given special attention.

The plant management shall set an example of safety-directed acting and actively support the latter.

1 (3) Integrated management system (IMS)

The prime objectives of the IMS are

a) the guarantee of safety,

b) the continual improvement of safety, and

c) the promotion of safety culture.

An IMS shall consider all objectives and requirements, such as safety, quality, ageing, staff safety, the environment, or profitability. All objectives and requirements have to be balanced, weighted and clearly specified in a comprehensible and transparent manner, giving consideration to the priority of safety. In this context, the interaction of human, technological and organisational factors (man-technology-organisation) has to be considered.

An IMS shall integrate all the requirements for a nuclear power plant resulting from laws, ordinances, standards and guidelines e.g. on safety, environmental protection, staff safety, quality, and finances.

The delineations and interfaces as well as the interplay and interactions within the IMS shall be specified and regulated such that the fundamental safety objective is not impaired by other business objectives.

All activities in the company and in the plant that are relevant for the operation of the plant shall be identified and systematically organised in processes. This also applies to activities of external personnel. Personnel capacity, competence and qualification shall be considered. The relations to external organisations shall be regulated correspondingly.

Regulations shall be made for at least the following processes:

- operation of the plant,
- planning, execution and evaluation of maintenance,
- modification of the plant and the operation,
- commissioning following modifications,
- organisational change,

- plant monitoring (physical monitoring, chemical and radiochemical monitoring, radiological monitoring),
- definition and implementation of protection requirements (fire protection, physical protection, IT security),
- planning and implementation of the internal accident management,
- qualification and training of the personnel,
- planning and implementation of materials management,
- handling of fuel assemblies and other core components,
- handling of radioactive waste,
- execution of the operational experience feedback,
- planning and execution of internal and external communication,
- management and execution of projects,
- execution of safety analyses and reviews,
- execution of documentation.

The interfaces between man, technology and organisation shall be considered in the development of the IMS.

In terms of continual improvement, the PDCA (Plan-Do-Check-Act) cycle shall be applied to all relevant operational activities, sub processes and processes and to the management system as a whole. The effectiveness of the management system shall be ensured by direct process evaluations and by process-independent evaluations.

If processes are supported by information processing systems (operational management systems), like e.g. in the elimination of disturbances and deficiencies, maintenance, or the isolation of systems, these shall be introduced in a quality-assured manner. According to their respective safety significance, they shall be regularly and systematically reviewed and adapted, if necessary.

The management system shall be systematically documented. Regarding the information contained, this documentation shall be complete, unambiguous and in itself consistent.

Suitable provisions shall be taken to obtain the competent engineering and technical support, provided by external contractors, in all safety-relevant areas over the entire operating lifetime of the plant.

The management system shall be suitable for providing early indications of a possible impairment of safety.

2 Technical safety concept

2 (1) In order to meet the radiological safety objectives (see Section 2.5), the radioactive materials present in the nuclear power plant shall be multiple confined by technical barriers and/or retention functions (see Section 2.2), and their radiation shall be sufficiently shielded. The effectiveness of the barriers and retention functions shall be ensured by the fulfilment of fundamental safety functions (see Section 2.3). A defence-in-depth concept shall be realised that ensures the fulfilment of the fundamental safety functions and the preservation of the barriers and retention functions on several consecutive levels of defence as well as in the case of any internal and external hazards (see Sections 2.1 and 2.4).

2.1 Defence-in-depth concept

2.1 (1) The confinement of the radioactive materials present in the nuclear power plant as well as the shielding of the radiation emanating from them shall be ensured.
In order to achieve this objective, a safety concept shall be implemented in which measures and equipment are allocated to different levels of defence. The levels of defence 1 to 4a are characterised by the following plant conditions:

- Level of defence 1:
  normal operation (specified normal operation, undisturbed)
- Level of defence 2:
  anticipated operational occurrences (specified normal operation, incident)
- Level of defence 3: accidents
- Level of defence 4a: very rare events

By the measures and equipment for quality assurance, the prevention of events and the control of events to be installed on these levels of defence as well as by the design against internal and external hazards as well as against human-induced external hazards (see Section 2.4), comprehensive and reliable protection from the radioactive materials present in the nuclear power plant shall be achieved.

Furthermore, additional measures and equipment to identify and limit the consequences of plant conditions that are not allocated to the above- mentioned levels of defence due to their low probability of occurrence shall be provided to an adequate extent as a precaution. Therefore, measures and equipment of the internal accident management shall be provided and planned in supplement on levels of defence 4b and 4c of the defence-in-depth concept. These levels of defence are characterised by the following plant conditions:

- Level of defence 4b: events involving the multiple failure of safety equipment
- Level of defence 4c: accidents involving severe fuel assembly damages.

2.1 (2) For accidents involving severe fuel assembly damages, measures shall be planned to support the external accident management in order to assess the consequences of accidents with potential or actually occurred releases of nuclear materials into the environment and to mitigate as far as possible their effects on man and the environment.

2.1 (3a) The safety concept on levels of defence 1 to 4b is aimed at prevention. Measures and equipment shall be provided which

- on level of defence 1
  - avoid abnormal operation,
- on level of defence 2
  - control abnormal operation,

- avoid the occurrence of accidents,

– on level of defence 3

- control accidents,
- prevent events involving the multiple failure of safety equipment,

– on level of defence 4a

- control very rare events.

On level of defence 4b, preventive measures of the internal accident management shall be provided so that there will be no severe fuel assembly damages in the case of an event involving the multiple failure of safety equipment.

2.1 (3b) On level of defence 4c, mitigative measures of the internal accident management shall be provided for accidents involving severe fuel assembly damages for the purpose of maintaining - by using all available measures and equipment - the integrity of the containment for as long as possible, excluding or limiting releases of radioactive materials into the environment according to subsection 2.5 (1), and achieving a long-term controllable plant state.

If spent fuel is stored in the spent fuel pool outside the containment, mitigative measures of the internal accident management shall be provided for the purpose of maintaining - by using all available measures and equipment - the integrity of the surrounding structural cover for as long as possible, excluding or limiting releases of radioactive materials into the environment according to subsection 2.5 (1), and achieving a long-term controllable plant state.

2.1 (4) The defence-in-depth concept shall be implemented for all plant states of power operation, low-power and shutdown operation, taking into account the respective representatively enveloping plant state parameters.

2.1 (5) The safety system as well as the emergency equipment shall be designed such that they will remain effective in the event of internal and external hazards.

Impacts resulting from very rare human-induced external hazards must not lead to safety equipment failures in such a way that the necessary safety functions are no longer effective; otherwise, specially designed equipment shall be provided for this case so that event sequences of level of defence 4b are prevented.

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

Measures and equipment that have to be effective on all or on several of these levels of defence shall be designed according to the requirements applicable to the level of defence with the respective most stringent requirements.

2.1 (7) It shall be ensured by the defence-in-depth concept 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 equipment on the next level.

2.1 (8) Using measures and equipment provided on levels of defence 2 or 3 to show that requirements of previous levels of defence are met is permissible if

– no other technical solutions can reasonably be achieved and

– no negative effects on the reliability and effectiveness of the measures and equipment used for the control of events need to be assumed.

2.1 (9) According to Sections 4.3 and 4.4, measures of the internal accident management shall be planned in such a way that they are effective for a broad spectrum of events involving the multiple failure of safety equipment and for phenomena occurring in connection with accidents involving severe fuel assembly damages.

2.1 (10) On level of defence 4, apart from the measures and equipment provided specially for this level, suitable respective measures and equipment of level of defence 1 to 3 may also be used.

2.1 (11) The measures and equipment provided specially for internal accident management on levels of defence 4b and 4c must not be used for demonstrating safety on the other levels of defence.

2.1 (12) The measures and equipment of all four levels of defence as well as the measures and equipment needed for internal and external hazards as well as for human-induced external hazards shall principally be available in line with the requirements of the respective operational modes. Any unavailabilities of safety-relevant equipment shall be limited in time depending on the operational modes and their safety-related effects. The corresponding conditions that have to be fulfilled shall be specified.

2.1 (13) The measures and equipment of levels of defence 1 to 4a as well as the measures and equipment needed for internal and external hazards as well as for human-induced external hazards shall meet stringent requirements with regard to the quality and reliability of planning, implementation and execution of the measures and the design, manufacturing, construction and operation of the equipment. The requirements for quality and reliability are guided by the safety significance of the measures and equipment.

Graded requirements apply for the measures and equipment provided specially for levels of defence 4b and 4c.

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 shall be ensured by sequential barriers and retention functions.

Note:
In the following, barriers are understood to be the fuel rod cladding, the reactor coolant pressure boundary, and the containment. The opening of valves in the reactor coolant pressure boundary per design does not mean an ineffectiveness of this barrier.

Retention functions are measures or equipment for the retention of radioactive materials, e.g. by filtering, water coverage, directed flow through maintaining low pressure, delay lines, building seals, drain pans, vessels or other confinements.

Maintaining a sufficient effectiveness of the barriers is furthermore essential for maintaining cooling and the coolability of the fuel assemblies.

The barriers shall be designed such that - as far as technically feasible - they are independent of each other in a way that in an accident or upon an internal or external hazard, one barrier will not fail as a consequence of the failure of another barrier.

The barriers and retention functions shall altogether be designed in such a way and maintained in such a condition over the entire plant service life that, in combination with the measures and equipment of the respective levels of defence, the respective safety-related acceptance targets and acceptance criteria (see Annex 2) as well as the radiological safety objectives according to Section 2.5 are met on the different levels of defence for all events or plant conditions and the associated mechanical, thermal, chemical and radiation- induced impacts.

The barriers and retention functions in their entirety shall also be reliably effective enough in all events resulting from internal and external hazards or very rare

human-induced external hazards that the radiological safety objectives according to Section 2.5 are fulfilled.

2.2 (2) If barriers are ineffective due to planned operational processes, other measures and equipment shall be available to achieve the radiological safety objectives (see subsection 2.5 (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 shall be 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, not considering permissible operations-induced cladding failures,

2. the reactor coolant pressure boundary, unless the reactor coolant system has been opened intentionally, and

3. the containment, unless it has been opened intentionally. The intentional opening of the containment shall not be performed before reaching specified pressure and temperature conditions in the reactor coolant system. It shall be ensured that the barrier can be restored at short notice in the event of a challenge or that effective and reliable retention functions are available so that an inadmissible release of radioactive materials is prevented or stopped in time.

b) for the confinement of the radioactive materials in irradiated fuel assemblies that are handled or stored within the plant:

1. during operational modes A to F (for definitions see Annex 2), the fuel rod cladding, not considering permissible operations-induced cladding failures, as well as

2. the containment, unless it has been opened intentionally. If spent fuel assemblies are handled or stored outside of the containment or if the containment has been opened intentionally, the lack of this barrier shall be compensated by retention functions.

The safe controlled confinement of the radioactive materials elsewhere in the plant shall be ensured in all operational modes by retention functions.

2.2 (4) On level of defence 3, the following barriers shall be 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 has been opened intentionally and its failure is postulated as initiating event,

3. the containment, unless it has been opened intentionally. If the containment has been opened intentionally, it shall be ensured that the barrier function of the containment can be restored in due time to the necessary extent or that effective and reliable retention functions are available so that an inadmissible release of radioactive materials is prevented or stopped in time.

b) for the handling and storage of fuel assemblies:

1. the fuel rod cladding, not considering event-specific postulated cladding failures) as well as

2. the containment, unless it has been opened intentionally. If the containment has been opened intentionally, it shall be ensured that the barrier function of the containment can be restored in due time to the necessary extent in the case of events involving releases of radioactive materials within the containment.

   If spent fuel assemblies are handled or stored outside of the containment, the lack of this barrier shall be compensated by retention functions.

   The achievement of the radiological safety objectives with regard to radioactive materials elsewhere in the plant shall be ensured in all operational modes by retention functions.

2.2 (5) On level of defence 4a, the following barriers shall be maintained effective apart from the necessary retention functions with regard to the confinement of the radioactive materials and the coolability of the reactor core:

1. the fuel rod cladding to the extent necessary for achieving the applicable acceptance targets,

2. the reactor coolant pressure boundary,

3. the containment.

2.2 (6) On level of defence 4b, apart from the retention functions for the activity inventory of the reactor core, at least one of the still existing barriers shall be maintained by the planned measures of the internal accident management to achieve the radiological safety objectives according to subsection 2.5 (1).

For the confinement of the radioactive materials in spent, stored fuel assemblies, the integrity of at least one barrier shall be ensured on level of defence 4b. If spent fuel assemblies are handled or stored outside of the containment, the lack of this barrier shall be compensated by retention functions (see subsection 2.2 (4)).

2.2 (7) Regarding level of defence 4c, subsection 2.1 (3b) applies.

2.3 Fundamental safety functions

2.3 (1) By the measures and equipment provided according to subsection 2.1 (3a) and taking into account the further requirements of Section 2.1, the following fundamental safety functions shall be achieved for the requirements 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 requirements shall be fulfilled:
For reactivity control:

- reactivity changes shall be restricted to admissible values,

- it shall be possible to shut down the reactor core and keep it subcritical in the long term,
- subcriticality shall be ensured during the handling and storage of fresh and spent fuel assemblies;
- For fuel cooling:
- coolant and heat sinks shall always be sufficiently available,
- heat transfer from fuel to heat sink shall be ensured,
- heat removal from the spent fuel pool shall be ensured;
- For the confinement of the radioactive materials:
- the mechanical, thermal, chemical and radiation-induced impacts resulting on the different levels of defence for the barriers or retention functions shall be limited such that their effectiveness regarding the achievement of the radiological safety objectives according to Section 2.5 is maintained
- it shall be possible to establish the barrier functions of the reactor coolant system and the containment adequately quickly if need be.

2.3 (3) On level of defence 4b, the long-term re-establishment of the fundamental safety objectives mentioned in subsection 2.3 (2) shall be achieved by measures of the internal accident management.

2.3 (4) Regarding level of defence 4c, subsection 2.1 (3b) applies.

2.4 Protection concept against internal and external hazards as well as against very rare human-induced external hazards

2.4 (1) All equipment that is necessary for shutting the reactor down safely, for maintaining it in shutdown condition, for removing the residual heat or for preventing a release of radioactive materials shall be designed such and be able to be maintained in such a condition that they fulfil their safety-related functions even in the case of internal and external hazards as well as very rare human-induced external hazards (see Annex 3).

Note:
Requirements for this equipment that have to be fulfilled regarding disruptive actions or other interference by third parties are not the subject of the "Safety Requirements for Nuclear Power Plants".

If any specific requirements apply regarding internal or external hazards with respect to the achievement of radiological safety objectives, these are listed in Annex 3 in connection with the hazards concerned.

2.4 (2) It shall be ensured that events resulting from external and internal hazards or from very rare human-induced external hazards that might inadmissibly impair the specified functioning of safety equipment are either prevented or adequately limited in their consequences according to subsection 2.1 (5). Here, above all passive equipment shall be provided. If passive equipment does not provide an adequately reliable prevention of inadmissible consequential effects, reliable active measures shall be provided.

2.4 (3) The subsystems of safety equipment that are redundant to each other shall be set up physically separate from each other or shall be protected such that in the event of an internal hazard, a redundancy-wide loss of function is prevented.

2.4 (4) All safety equipment shall be designed such and be kept permanently in such a condition that they fulfil their safety-related functions even in the event of an external hazard.

2.4 (5) Regarding any impacts from very rare human-induced external hazards, the last paragraph of Section 2.1 (5) applies.

2.5 Radiological safety objectives

2.5 (1) On levels of defence 1 and 2

- radiation exposure of the personnel shall be kept as low as achievable for all activities, even below the limits of the Radiation Protection Ordinance, taking into account all circumstances of each individual case,
- any discharge of radioactive materials with air or water shall be controlled via the specially provided discharge paths; the discharges shall be 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 shall be kept as low as achievable, even below the limits of the Radiation Protection Ordinance, taking into account all circumstances of each individual case.

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 removal of their consequences shall 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 shall not exceed the relevant accident planning levels of the Radiation Protection Ordinance,
- any release shall only happen via specially provided release paths; the release shall be monitored and shall be documented and specified according to its kind and activity; and
- the on-site and off-side radiological consequences shall be kept as low as possible, taking into account all circumstances of each individual case.
- On level of defence 4
- the planning of activities to control events of level of defence 4a as well as for the planning of activities in connection with internal accident management measures shall be based the relevant requirements of the Radiation Protection Ordinance regarding the anticipated radiation exposure of the personnel,
- the monitoring of releases of radioactive materials from the plant according to their kind and activity shall be ensured and
- the on-site and off-side radiological consequences shall be kept as low as possible, taking into account all circumstances of each individual case.

Taking into account the measures and equipment for the internal accident management provided on levels of defence 4b and 4c,

- any releases of radioactive materials into the environment of the plant, caused by the early failure or bypass of the containment and requiring measures of the external accident management for the implementation of which there is not sufficient time available (early release), or
- any releases of radioactive materials into the environment of the plant requiring wide-area and long-lasting measures of the external accident management (large release)

shall be excluded[1], or their radiological consequences shall be limited to such an extent that measures of the external accident management will only be required to a limited spatial and temporal extent.

2.5 (2) All safety-relevant equipment of a nuclear power plant shall be designed in such a way, maintained in such a condition and protected in such a manner against impacts of internal and external hazards as well as very rare human-induced external hazards that they fulfil their safety-related functions for meeting the requirements according to subsection 2.5 (1).

All equipment of a nuclear power plant that contain or may contain radioactive materials shall be conditioned, arranged and shielded in such a way that the relevant requirements according to subsection 2.5 (1) are met with regard to the radiation exposure of individuals for all necessary activities on levels of defence 1 and 2 as well as for the planning of activities to control events on levels of defence 3 and 4a and in the case of internal and external hazards, very rare human induced external hazards and within the framework of internal accident management measures.

[1] The occurrence of an event or event sequence or a state can be considered as excluded if it is physically impossible to occur or if it can be considered with a high degree of confidence to be extremely unlikely to arise.

3 Technical requirements

3.1 General requirements

3.1 (1) In the design, manufacturing, construction and tests as well as during the operation and maintenance of the safety-relevant plant components, principles and processes shall be applied to comply with the special safety-related requirements of nuclear technology. Upon the application of acknowledged engineering practices, these shall be assessed case-by-case with regard to whether they comply with the state of the art in science and technology in the respective case of application.

3.1 (2) Safety-enhancing design, manufacturing and operating principles shall be applied to the measures and equipment on levels of defence 1 to 4a as well as the measures and equipment needed for internal and external hazards as well as for as well as the measures and equipment needed for internal and external hazards as well as for human-induced external hazards with regard to all operational modes (see also subsection 2.1 (13)). In particular, the following shall be implemented:

a) well-founded safety factors in the design of components depending on their safety significance; here, established rules and standards may be applied with regard to the case of application;

b) preference to inherently safe-acting mechanisms in the design;

c) use of qualified materials and manufacturing and testing methods and of equipment that has been proven by operating experience or which has been sufficiently tested;

d) maintenance- and test-friendly design of equipment, with special consideration of the radiation exposure of the personnel;

e) ergonomic design of the workplaces;

f) assurance and maintenance of the quality features during manufacturing, construction and operation;

g) execution of regular in-service inspections to an extent that is necessary from a safety-related point of view;

h) reliable monitoring of the relevant operating states in the respective operational modes;

i) preparation and implementation of a monitoring concept with monitoring systems to detect and control operation- and ageing-induced damages;

j) recording, evaluation and safety-related use of operating experience.

3.1 (3) To ensure sufficient reliability of the equipment of level of defence 3 (safety equipment), the following design principles shall be applied in addition to sub-section 3.1 (2):

a) redundancy;

b) diversity;

c) segregation of redundant subsystems, unless this is 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 equipment;

g) the auxiliary and supply systems of the safety equipment shall be designed with such reliability that they ensure the required high availability of the equipment to be supplied;

h) automation (in the accident analysis, equipment that has to be actuated manually shall in principle not be credited until 30 minutes have passed).

3.1 (4) Quality and reliability of all equipment of the nuclear power plant shall correspond to their respective safety significance.

All safety-relevant equipment shall be classified according to its safety significance. The criteria for quality and reliability applicable in the specified classes shall be defined and shall include, in particular, specifications on requirements with regard to design, manufacturing, ambient and effectiveness conditions, emergency power supply and long-term maintenance of quality.

1. Of high safety significance and accordingly classified shall be:

   a) equipment whose failure leads to event sequences that cannot be controlled,

   b) equipment that is necessary for accident control, including the auxiliary and supply systems required for it, and

   c) emergency equipment.

2. Of graded safety significance and accordingly classified shall be:

   a) equipment that is necessary for accident prevention, including the auxiliary and supply systems required for it,

   b) equipment for compliance with and monitoring of defined radiological limits, particularly by maintaining the required effectiveness of barriers and retention functions,

   c) other equipment performing safety significant functions,

   d) equipment of the internal accident management.

3.1 (5) The potentials for common-cause failures of safety equipment shall be analysed. Provisions to reduce the probability of occurrence of such failures shall be taken in such a way that a multiple failure of safety equipment on level of defence 3 need not be assumed. Redundant safety equipment for which possible common-cause failures have been identified, shall be installed in diverse manner as far as technically reasonable.

3.1 (6) The reliability and effectiveness of safety functions of level of defence 3 shall be ensured by measures and equipment, including their auxiliary and supply systems,

- 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 station service power supply, and

– for loss of functions or unavailabilities according to the single-failure concept as outlined in subsection 3.1 (7).

Sufficient margins shall exist between operational limit values and the limit values that trigger safety equipment so that undesired frequent activation will not take place. Limit values that trigger safety equipment shall be chosen conservatively in order to take uncertainties in the safety analyses into account.

3.1 (7) The safety equipment necessary for the control of events on level of defence 3 shall be available redundantly and segregated in such a way that the safety functions necessary for controlling events are still sufficiently effective if it is postulated that, in the event of their required function,

– a single failure of a safety equipment with the most unfavourable effects occurs due to a random failure, and

– there is at the same time an unavailability of a safety equipment due to maintenance measures with the most unfavourable effects in combination with a single failure.

Single failures are generally postulated for active as well as for passive equipment, exceptions shall be justified.

Note:
More detailed requirements for the application of the single-failure concept are contained in Annex 4 "Principles for the Application of the Single-Failure Concept and for Maintenance". Annex 4 furthermore also contains requirements for the planning and implementation of maintenance measures as far as these are relevant for the application and effectiveness of the single-failure concept.

3.1 (8) In operational modes in which parts of safety equipment need not be available according to the plant operating rules, the reliable and effective control of the events to be assumed in these shall be ensured also under these conditions.

3.1 (9) Human-induced external hazards
Regarding human-induced external hazards, it shall be ensured that in case of such an event, at least one of the redundant equipment necessary for event control will remain available. Here, consequential impacts shall also be taken into consideration.

In case of human-induced external hazards, the autarchy of the safety functions to ensure electrical power supply and all cooling and operating agents that are necessary to take the plant to a controlled state and maintain it in this condition for at least 10 hours.

The emergency equipment shall have no adverse safety-related effects on measures and equipment of level of defence 3.

3.1 (10) Internal accident management
Internal accident management shall comprise preventive and mitigative accident management measures as well as severe accident management guidelines for an emergency response staff to be formed in case of a severe accident.

The equipment provided for accident management measures must impair neither normal specified operation nor the use of safety and emergency equipment as specified by their design. Their compatibility with the safety concept shall be ensured.

The accident management measures rest on specially dedicated measures and equipment including equipment that is not permanently installed (mobile) as well as on the flexible use of available safety equipment, operating systems and emergency equipment.

The operability of the equipment provided for accident management measures shall be ensured by maintenance and in-service inspections.

3.1 (11) The measures and equipment of the accident management shall remain effective even in case of internal and external hazards as well as in case of human-induced external hazards if these hazards may lead to multiple failures of safety equipment that is necessary in these situations and if these measures and equipment contribute to the mitigation of the effects of the respective hazards and human-induced external hazards.

3.1 (12) Inspection and maintenance

All safety-relevant equipment shall be 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.

The function of safety-relevant equipment shall be tested to the extent necessary under conditions that resemble a challenge in the best-possible way.

3.1 (12a) If for certain equipment it is not possible to perform state-of-the-art in-service inspections to the extent necessary to detect possible deficiencies, it shall be 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, that a manufacturing documentation is available and that no irregularities or deviations from requirements to be fulfilled can be derived from it.

3.1 (12b) In the case of such restricted testability, measures and equipment shall be provided for the control of the possible consequences of these deficiencies, to be postulated notwithstanding the provisions according to subsection 3.1 (12a), in such a way as 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 (13) Requirements for the ergonomic design of the prerequisites for reliable personnel actions

a) All foreseeable activities and measures with safety relevance in the plant on levels of defence 1 to 4 shall be designed with consideration of ergonomic aspects in such a way that the prerequisites for the necessary safety-related behaviour of the persons active in the plant are given. This also applies to activities that have to be carried out in connection with internal or external hazards as well as with human-induced external hazards. Regarding levels of defence 4b and 4c, the requirements relate to feasibility, accessibility and radiation protection.

b) The principle according to subsection 3.1 (13) a) shall also be applied to the design of all workplaces where these activities are carried out and to all working tools that are intended to be used for these activities. The pathways provided along which the personnel reach the job site with all necessary working tools shall also be taken into account.

Note:
Working tools include among other things: information, operation and communication equipment, measuring and testing devices, instruments and other equipment, means of transport, hoists and load attachment rigging as well as documents with instructions and other information on jobs to be done.

c) In the implementation of the principle according to subsection 3.1 (13) a), all influences to which those staff members carrying out these activities at the workplace and on the provided pathways to the job site may be exposed shall be taken into account. These include i.a. radiation exposure, indoor climate, lighting and noise exposure.

d) The principle according to subsection 3.1 (13) a) shall also be applied to the design of the work processes, the distribution of tasks between man and machine, the division of labour among the persons carrying out these activities.

3.2 Requirements for the reactor core and the shutdown systems

3.2 (1) The control of reactivity in the reactor core shall be ensured for all operational modes on levels of defence 1 to 4a as well as in the case of internal and external hazards and under very rare human-induced external hazards.

3.2 (2) The reactor core, the relevant equipment for the monitoring, control and limitation of reactor power and for reactor shutdown shall be designed, manufactured and maintained in such a condition that in combination with the cooling systems for the reactor core, the respective design limits of levels of defence 1 to 4a are not exceeded.

3.2 (3) The reactor core shall be designed such that due to inherent reactor-physical feedback characteristics the fast reactivity increases to be considered are limited to such a degree that in combination with the other inherent characteristics of the plant and the limitation or 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 shall be designed such that due to inherent reactor-physical feedback characteristics the anticipated transients with postulated failure of the fast-acting shutdown system (reactor scram system) to be considered on level of defence 4a (ATWS) are limited to such a degree that in combination with other measures and equipment 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 shall have

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

The control or 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 shall 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 rod element is ineffective, and
- in the case of internal and external hazards and under very rare human-induced external hazards so that the respective safety-related acceptance targets and acceptance criteria are met.

Note:
In case of events on level of defence 3, the postulated ineffectiveness of the most reactivity-effective control rod element may be treated as single failure according to subsection 3.1 (7) with regard to the subcriticality to be maintained.

3.2 (7) It shall be possible to render the reactor subcritical and keep it in a stable subcritical state in the long run on levels of defence 1 to 4b as well as in the case of internal and external hazards and under very rare human-induced external hazards, 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.

In PWRs, the equipment for injecting soluble neutron absorbers into the coolant in the case of conditions or events of levels of defence 1 to 4a as well as regarding internal and external hazards and under very rare human-induced external hazards shall be able on its own to provide the required amount of subcriticality.

In BWRs, the following equipment shall each alone be able to provide the required amount of subcriticality:

- in the case of conditions or events of levels of defence 1 to 4a as well as regarding internal and external hazards and under very rare human-induced external hazards, the electromagnetic insertion of the control rod elements, and
- under the conditions of level of defence 1, the equipment for injecting soluble neutron absorbers into the coolant.

If the lasting continuation of subcriticality on levels of defence 1 to 3 is ensured by control rod elements alone, the ineffectiveness of the most effective control rod element shall be postulated.

Note:
On level of defence 3, this can be treated like a single failure according to subsection 3.1 (7).

3.3 Requirements for the equipment for fuel cooling in the reactor core

3.3 (1) Fuel cooling (heat removal from the reactor core) shall be ensured in all operational modes on levels of defence 1 to 4a as well as in the case of internal and external hazards and under very rare human-induced external hazards.

For this purpose, the heat produced in the fuel assembly shall be removed such that the safety-related acceptance targets and acceptance criteria for the fuel assemblies and the other safety-relevant equipment applicable on the respective levels of defence are met during their entire service life.

3.3 (2) Equipment shall be available by means of which during normal operation

a) the reactor can be started up and shut down reliably and according to the requirements, and

b) the residual heat can be removed reliably and according to the requirements also under consideration of all operational modes during refuelling and, if required, the simultaneous cooling of the spent fuel assemblies in the fuel pool as well as during maintenance measures.

3.3 (3) A reliable and redundant system for emergency cooling of the reactor core (emergency core cooling system) in case of a loss-of-coolant accidents shall be provided that ensures for the break sizes, break locations, operating states and accident-induced transients in the reactor coolant system to be considered that

a) the safety-related tasks are fulfilled also with respect to the requirements of subsection 3.1 (7),

b) the respective applicable safety-related acceptance targets and acceptance criteria for the fuel assemblies, the core internals and for the containment are met.

3.3 (4) A reliable and redundant system for reactor shutdown and residual-heat removal in case of accidents without loss of coolant and after internal and external hazards shall be 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 requirements of subsection 3.1 (7).

3.3 (5) Even in case of a loss of the primary heat sink as a result of loss of functions in the area of the circulating water intakes and returns, residual-heat removal from the plant shall be ensured under all operating states by a diverse heat sink (possibly also by different heat sinks in combination). The equipment needed for this purpose shall satisfy at least the requirements for internal accident management measures; their effectiveness shall be demonstrated.

The availability of this diverse heat sink shall also be ensured in the event of external hazards.

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

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

3.4 (2) For this purpose, an adequate safety factor, justified from a safety point of view, shall be added in the design to the determined values of impacts according to the requirements of subsection 3.1 (2) to ensure that the specified limit values for the loads on the reactor coolant pressure boundary resulting from impacts under specified normal operating and accident conditions are not exceeded.

3.4 (3) For the reactor coolant pressure boundary and the pressure-retaining walls of components of the external systems with nominal diameters of more than NB 50, basis safety shall be ensured by fulfilment of the following requirements 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.

Note:
In case of the realisation of this basis safety, catastrophic failure of these plant components as a result of manufacturing defects is not to be postulated.

A concept to maintain component integrity shall be put up to assure and evaluate the requisite quality of these components in operation. For this purpose, additional measures and equipment for the monitoring of causes and effects of damage mechanisms, in particular of leakages during operation shall be specified and installed.

3.4 (4) For the reactor coolant pressure boundary and the pressure-retaining walls of components of the external systems, leak and break postulates shall be 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 needs not be postulated, restricted leak and break postulates may be used. For these piping systems and components, a high level of confidence shall be demonstrated regarding the impacts on these systems from levels of defence 1 to 4a, in the case of internal and external hazards as well as under very rare human-induced external hazards.

It shall be additionally demonstrated for these selected piping systems and components that under these impacts conditions, faults in the pressure- retaining walls cannot lead to a leak or break of the pipe or component which put the applied limited leak and break assumptions into question. In doing so, credit may be taken of generic proofs and results of experimental studies if the components are basically safe designed. Furthermore, regarding valve and pump housings, enveloping safety verifications are permissible for the housings including the nozzle areas for connecting piping. Adherence to the applicable boundary conditions during operation shall be verified by suitable measures for the examination of the impacts and by non-destructive in-service inspections of the component.

3.4 (5a) For preventing the admissible pressure in the reactor coolant pressure boundary (for PWRs including the secondary side of the steam generator) from being exceeded, effective and reliable equipment for pressure limitation and overpressure protection shall be provided.

3.4 (5b) Equipment for primary depressurisation shall be provided with which internal accident management measures aimed at depressurisation can be effectively carried out so that there will be no core meltdown under high pressure.

3.4 (6) The nuclear power plant shall be 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 nor in the case of internal and external hazards and very rare human-induced external hazards. Here, the safety factors specified according to the requirements of subsection 3.1 (2) shall be considered.

3.4 (7) The components of the reactor coolant pressure boundary and the external systems shall be arranged and anchored such that if they were affected by events on levels of defence 3 and 4a as well as in the case of internal and external hazards and very rare human-induced external hazards, no consequential damage can be caused to other safety-relevant plant components that would jeopardise the fulfilment of the safety functions necessary to control the event.

3.5 Requirements for structures

3.5 (1) The structures shall be designed and maintained in such a condition that they contribute to

- ensuring the load transfer specified for the respective level of defence of the systems and components on levels of defence 1 to 4a and in the event of external or internal hazards as well as under very rare human-induced external hazards,
- ensuring protection against these hazards,
- shielding of the ionising radiation and the retention of radioactive materials, and
- fire and lightning protection of the plant to the

respectively necessary extent.

3.6 Requirements for the containment system

3.6 (1) The nuclear power plant shall have a containment system consisting of the containment and the surrounding building as well as of the auxiliary systems for the retention and filtering of any possible leakages from the containment.

The containment system shall fulfil 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.

Under the operating conditions in which it is closed according to schedule, the containment shall fulfil its safety functions on levels of defence 1 to 3 as well as during transients involving the failure of reactor scram (level of defence 4a) and in the event of internal and external hazards as well as under very rare human-induced external hazards.

In operational modes during which the containment may be open according to schedule, it shall be ensured that under the conditions of level of defence 1 and the events postulated on levels of defence 2 and 3 and in the event of internal and external hazards as well as under very rare human-induced external hazards, effective and reliable retention functions are available and an inadmissible release of radioactive materials from the containment is prevented or stopped in due time.

3.6 (2) Devices containing radioactive materials shall be installed within the containment system unless an inadmissible release of radioactive materials into the environment can be prevented otherwise.

Plant components under high pressure and containing reactor coolant shall on principle be installed inside the containment. Main-steam and feedwater line as well as other piping sections may be exempted from this principle if this is necessary from a technical point of view and if it is ensured that the rupture of such piping will not lead to any inadmissible radiation exposure in the environment.

3.6 (3) Reliable, sufficiently fast and adequately long-lasting isolation of the containment penetrations shall be ensured.

The required leak-tightness for the containment shall be quantified by a maximum permissible leak rate for the operational modes in which the containment is closed.

3.6 (4) The containment shall be surrounded by a building. The building shall be designed such that the space between containment and building can be kept at sufficiently low pressure in the long term during operational modes with closed locks even in the case of conditions of events on level of defence 3 prevailing inside the containment. For this purpose, there shall be structural provisions for the surrounding building that ensure air-tightness. It shall be possible to vent the interspace via the stack and, if required, via filters. Inspections of safety-relevant plant components shall be possible.

3.6 (5) The containment shall be protected by structural decoupling such that any load transfers in the case of very rare human-induced external hazards will not lead to an impairment of its function. Likewise, the stability or integrity of internals and rooms shall be maintained as far as necessary in all events of level of defence 3 and upon internal and external hazards, including the effect of pressure differences.

3.6 (6) The surrounding building shall shield the outside from direct radiation to a sufficient degree and shall protect the containment and its internals against impermissible consequences from the external hazards and very rare human-induced external hazards to be considered for the plant.

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

3.6 (8) For accidents involving severe fuel assembly damages (level of defence 4c), the following shall apply additional to the requirements of subsection 2.1(3b):

- It shall be ensured by internal accident management measures that there will be no overpressure failure of the containment due to a steady pressure increase. If containment venting is provided as an intentional accident management measure, this shall be effective under the expected severe accident conditions and shall provide efficient filters for aerosol and iodine retention. Containment failure due to negative pressure as a result of venting shall be avoided.
- In the event of an accident involving severe fuel assembly damages, it shall be achieved by internal accident management measures that there will be no deflagration processes of gases (H_2, CO) inside the containment that will put containment integrity at risk.
- In the event of an accident involving severe fuel assembly damages in the spent fuel pool, it shall be achieved by internal accident management measures that there will be no combustion processes of gases (H_2,) that will put containment integrity or the integrity of the structure surrounding the spent fuel pool at risk.

3.7 Requirements for instrumentation and control

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

3.7 (2) The nuclear power plant shall be equipped with instrumentation and control equipment with instrumentation and control 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 shall be equipped with reliable instrumentation and control system equipment with instrumentation and control functions on level of defence 3 (reactor protection system) whose instrumentation and control functions initiate protective actions as soon as defined safety limits are reached.

This equipment shall be designed according to the following principles:

- redundant design of components, subassemblies and sub-systems,
- diversity (see subsection 3.1 (5)),
- physical separation of equipment corresponding to the impact range of possible postulated initiating events,
- automatic failure monitoring,
- adaptation of the components to the possible ambient conditions,
- simple software structure,

- limitation of the functional scope of the hardware and software to the necessary safety-related degree, and
- use of fault-preventing, fault-detecting and fault-controlling measures and equipment.

Notes:
For computer-based or programmable instrumentation and control equipment, there will also be future requirements made by the Security Regulations, which also contain design requirements. The demonstrable fulfilment of all security requirements is a prerequisite for the licensing of these systems.

Accordingly, computer-based or programmable instrumentation and control equipment will only be used on level of defence 3 if it can be verified for their entire life cycle that any manipulation of this equipment is prevented by suitable measures of design or security or if it is prevented that that manipulations of individual or various different computer-based or programmable equipment will have an effect on the safety of the plant.

3.7 (4) In the design of the instrumentation and control equipment according to subsection 3.7 (3), the potentials and the effects of systematic failures of instrumentation and control equipment on the event sequences on level of defence 3 shall be analysed, taking the process-related requirements into account.

Provisions shall be taken against systematic failures to reduce their probability of occurrence in such a way that they no longer need to be postulated on level of defence 3.

3.7 (5) Manual reactor scram shall be possible at any time during operational modes in which the availability of the reactor scram system is required, even in case of a postulated systematic failure of computer-based instrumentation and control equipment including systematic software failure.

The manual actuation of protective actions shall be devised independent of automatic instrumentation and control equipment.

3.7 (6) The instrumentation and control equipment according to subsection 3.7 (3) shall be designed in such a way that even if the postulated single failure occurs in this equipment, no actions will be triggered that could take the reactor to accident conditions or prevent accident control.

3.7 (7) Monitoring and alarm equipment shall be 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 state of the plant and the developing relevant processes and which are able to display and register all safety-relevant operating parameters.

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

3.7 (8) Specific instrumentation shall be available at the nuclear power plant which for event sequences and plant states on levels of defence 3 and 4 as well as in case of internal or external hazards as well as under human-induced external hazards.

a) provides sufficient information about the plant condition to be able to take the necessary protective actions for the personnel and the plant and to determine their efficiency,

b) allows the monitoring of the event sequence and the documentation of the events,

c) allows an estimation of the effects on the environment,

d) is supplied with electrical power for at least 10 hours (even if the battery-buffered electrical power supply is lost), and

e) performs and processes measurements redundantly.

The equipment for the registration and recording of the respective necessary information shall be diverse and accident-proof.

Regarding levels of defence 4b and 4c, sufficient information about the condition of the plant shall be provided to be able to take any accident management measure and to determine their effectiveness as well as to allow an estimation of their effects on the environment.

3.7 (9) On levels of defence 4b and 4c, accident management measures may have priority over competing actions of the lower levels of defence. Interventions into equipment fulfilling instrumentation and control functions on levels of defence 1 to 4a are acceptable if this is required by accident management measures in the event of a challenge.

3.7 (10) The functions to be performed by the instrumentation and control equipment shall be classified by their safety-significance according to subsection 3.1 (4). The requirements 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 subsystems) of the instrumentation and control equipment shall be defined according to the safety-related classification of the functions fulfilled by them.

No requirements are made in the "Safety Criteria for Nuclear Power Plants" for the instrumentation and control equipment fulfilling instrumentation and control functions that are not categorised.

3.7 (11) Unauthorised access to information systems and instrumentation and control systems of the plant shall be prevented. The effectiveness and reliability of the measures to be provided for this purpose shall correspond to the safety significance of the information systems and instrumentation and control systems.

3.8 Requirements for control rooms

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

3.8 (2) An supplementary control room shall be provided outside the main control room from where in the event of a loss of function of the main control room, including any adjacent rooms that 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 main control room and the supplementary control room shall be physically separated, independently power-supplied and protected against external hazards as well as against very rare human-induced external hazards in such a manner that they cannot be disabled at the same time.

3.8 (4) The main control room and the supplementary control room shall be designed with consideration of ergonomic aspects in such a way that the conditions for the necessary safety-oriented behaviour of the personnel are fulfilled.

3.8 (5) Suitable alerting equipment and means of communication shall be available that can be used for giving behavioural instructions to all persons present in the plant from at least one central location if events occur on any of the levels of defence.

3.8 (6) Escape routes shall exist for the rescue and escape of humans from all hazardous situations.

3.8 (7) The rooms planned for the emergency response staff shall be suitably equipped. The main control room and the rooms provided for the emergency response staff shall be accessible and available under the conditions expected in connection with events on levels of defence 4b and 4c as well as during the performance of planned accident management measures.

3.9 Requirements for the electrical power supply

3.9 (1) The electrical power supply of the nuclear power plant shall be designed such that the electrical power supply of the consumers executing functions on levels of defence 1 to 4a, during internal and external hazards as well as in case of human-induced external hazards is ensured in compliance with their electrical power supply conditions. The electrical power supply shall be designed of such reliability that it will not dominate unavailability of the supplied systems whose loss of function might lead to adverse safety-related effects.

3.9 (2) For this purpose, a minimum of two grid connections for the electrical power supply of the nuclear power plant shall be available. These grid connections shall be functionally separated from each other and decoupled regarding their protection. If the circuit-breakers of the grid connections between the power plant and the grid are not in the responsibility of the licensee, the licensee shall ensure by suitable measures that the design of the grid connections meets the safety requirements of the nuclear power plant.

In addition to the electrical power supply from the grid connections and the main generator, reliable emergency power supply facilities including diesel generators, batteries, rectifiers and converters shall be provided for the plant's safety system, emergency equipment and further equipment necessary for safety to ensure the electrical power supply of these systems in case of a loss of offsite power supply and of the main generator.

The emergency power supply facilities shall be constructed redundantly, physically separated, generally unmeshed, functionally independent of each other, and protected from each other. Thereby the degree of redundancy of the emergency power supply facilities shall correspond at least to the degree of redundancy of the process-based equipment to be supplied. The capacity of each battery of one redundant system train shall be designed such that a discharge time of at least two hours is ensured for events on levels of defence 2 to 4a.

Meshing of the individual trains of the emergency power supply facilities is acceptable in individual cases if it has been demonstrated that this will not impair the reliability of the emergency power system unacceptably. Here, special care shall be taken that none of the possible failures to be considered can lead to the failure of more than one train.

In addition to this, an electrical power supply option shall be provided, ensuring - independent of these power supply options - the electrical power supply for residual-heat removal by at least one redundant residual-heat removal train (emergency power grid connection).

3.9 (3) For the design of components that contain electrical, electromechanical or electromagnetic component parts as well as analogue electronic subassemlies with a simple structure, the potentials for systematic failures of these components shall be analysed. Provisions shall be taken to reduce the occurrence probability of systematic failures in a way that a systematic failure need no longer be

postulated or that the effects of systematic failures can be controlled.

For the design of components that contain complex electronic assemblies (programmable or non-programmable), fault-preventing or fault-controlling provisions shall be taken on component level and, if applicable, also fault-controlling provisions on system level so that redundancy-wide systematic failures on system level of the respective affected level of defence are prevented.

Note:
Simple means that the function as well as the failure behaviour of the component can be determined deterministically on the basis of the regularities of electrical engineering.

Complex means that the function as well as the failure behaviour of the component can no longer be determined deterministically on the basis of the regularities of electrical engineering.

3.9 (4) The electrical power supply necessary for the performance of the accident management measures shall be ensured for a period of 10 hours without any external support.

The re-establishment of the electrical power supply after a failure of the non-battery-buffered electrical power supply shall be ensured by measures and equipment of the internal accident management.

To ensure the electrical power supply in case of a longer-lasting unavailability of the above-mentioned grid connections or all external grids, substitute measures shall be provided in such a way that after three days at the latest it is possible to resume the supply of electrical power with their help. The equipment needed for this purpose shall be provided either within the area of the power plant or in the area close to the plant and shall be protected against external hazards. For this electrical power supply equipment, at least two adequate external connections shall be provided. These shall be designed and arranged in such a way that the substitute measures can be applied effectively in the above-mentioned cases.

The electrical power to be provided shall be sufficient to remove the residual heat in the respective plant condition with the help of the systems or the accident management measures with consideration of the requirements of subsection 2.5 (1).

3.10 Requirements for the handling and storage of the fuel assemblies

3.10 (1) On levels of defence 1 to 4a as well as in the case of internal and external hazards as well as under very rare human-induced external hazards, the control of reactivity during fuel assembly handling and storage shall be ensured for all operational modes.

3.10 (2) Measures and equipment for the handling and storage of non-irradiated and irradiated fuel assemblies shall be provided such that a criticality event in the storage facilities need not be postulated even under accident conditions as well as in the case of internal and external hazards and under very rare human-induced external hazards.

3.10 (3) Fuel cooling shall be ensured in all operational modes on levels of defence 1 to 4a as well as in the case of internal and external hazards and under very rare human-induced external hazards.

3.10 (4) Even in case of a loss of the primary heat sink as a result of loss of functions in the area of the circulating water intakes and returns, residual-heat removal from the spent fuel pool shall be ensured under all operating states by a diverse heat sink (possibly also by different heat sinks in combination). The equipment needed for this purpose shall satisfy at least the requirements for internal accident

management measures; their effectiveness shall be demonstrated.

The availability of this diverse heat sink shall also be ensured in the event of external hazards.

3.11 Requirements for radiation protection

3.11 (1) At the nuclear power plant, the personnel, organisational, spatial and equipment-related conditions shall be 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 shall be 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 shall be provided to allow adequately fast, precise and reliable environmental radiation protection monitoring on levels of defence 1 to 4 and in the case of internal and external hazards and under very rare human-induced external hazards to the necessary extent.

3.11 (4) Measures and equipment shall be 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 shall be designed such and this equipment shall be in such a condition and located and shielded such that any inadmissible radiation exposure of the plant's own and external personnel and the environment and any release of radioactive material into the environment is prevented.

In this connection, the number and duration of tasks of the personnel in radiation fields and the possibilities of personal contamination and incorporation shall be kept as low as achievable, taking into account all circumstances of each individual case.

3.11 (5) The design and operation of the plant shall be planned such that the accumulation of radioactive waste and of radioactive materials arising in the plant that can be utilised without any harm are kept as low as achievable regarding both their activity and amount, taking into account all circumstances of each individual case.

3.11 (6) In the planning of internal accident management measures, measures shall be included to reduce the expected radiological consequences, taking into account all circumstances of each individual case, if there are reasons to believe that there will be releases into the environment.

3.11 (7) The condition of nuclear power plants shall be such that they can be decommissioned in compliance with the radiation protection regulations. A concept shall exist 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 equipment to be realised according to subsection 2.1 (3) on levels of defence 1 to 3 shall be based on:

- the operating conditions to be expected on level of defence 1, including testing conditions,
- the events whose occurrence is anticipated on level of defence 2 during the operating lifetime of the plant,
- an enveloping spectrum of events on level of defence 3 whose occurrence is not to be expected during the operating lifetime of the plant due to the reliability and effectiveness of the measures and equipment provided, but which has to be postulated nevertheless.

4.1 (2) The respective measures and equipment shall be 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 (see Annex 2) are met, taking specified boundary conditions into account.

4.1 (3) The completeness and the enveloping character of the events to be considered shall be ensured plant-specifically.

Note:
See Annex 2 on this point.

4.1 (4) For defined events, there is the option of demonstrating that the occurrence of these events is prevented due to special precautionary measures. These events are marked separately in the event lists in Annex 2.

The quality of the precautionary measures to be taken shall be guided by the potential effects.

For events whose occurrence does not have to be postulated if special precautionary measures are provided, it shall be demonstrated that the requirements for effectiveness and reliability of the respective precautionary measures are fulfilled.

Note:
See Annex 2 on this point.

4.2 Internal and external hazards and very rare human induced external hazards

4.2 (1) The design of the equipment according to subsection 2.4 (1) shall be based on the following:

a) the respective most severe internal hazards or external hazards to be postulated;

b) the special characteristics of long-lasting external hazards;

c) combinations of several external hazards (e. g. earthquake, flood, storm, lightning) as well as of very rare human-induced external hazards between them or combinations of these hazards with internal events (e. g. pipe break, internal fires, loss of offsite power); these combinations shall be postulated if the combined events may show a causal relationship or if their simultaneous occurrence has to be considered due to their probability and the extent of the damage caused.

4.2 (2) The external hazards to be postulated as having the most severe consequences shall be those that have to be postulated site-specifically according to the state of the art in science and technology. Here, the foreseeable future development of the site properties regarding the external hazards to be postulated shall also be taken into account.

4.3 Events involving the multiple failure of safety equipment

4.3 (1) For the determination of the representative event sequences for the planning of preventive measures of the internal accident management, the results of deterministic and probabilistic safety analyses, operating experience as well as results of reactor safety research and international recommendations shall be referred to within the framework of an overall survey. Here, event sequences shall be considered which according to the results of probabilistic safety analyses make a dominant contribution to the core melt frequency and especially those that may lead to a direct release of radioactive materials into the environment.

4.3 (2) The plant-specific spectrum of event sequences on which the planning of preventive measures of the internal accident management shall be based shall comprise at least events from the following groups of events:

- transients,
- loss-of-coolant accidents inside the containment as a result of the maximum postulated leaks in the reactor coolant system,
- loss-of-coolant accidents with containment bypass, and
- external and internal hazards if these hazards can lead to multiple failures of safety equipment.

Based on a postulated multiple failure of safety equipment, the representative event sequences to be referred to for the planning shall be defined.

4.3 (3) For the planning of preventive measures of the internal accident management aimed at the restoration and maintenance of fuel cooling in the spent fuel pool, the following event sequences shall be postulated in particular:

- event sequences involving the complete loss of the systems provided on levels of defence 1 to 3 for heat removal from the spent fuel pool as well as
- event sequences involving a loss of coolant from the spent fuel pool and a drop below the minimum level required for the operation of the systems for heat removal.

4.3 (4) Regarding the event sequences mentioned under subsections 4.3 (2) and (3), the possibility of the complete loss of one each of the safety functions necessary for the control of events on level of defence 3 shall be analysed when planning preventive measures of the internal accident management. Here, the failure of the required safety equipment and, on the other hand, the loss of one each of the supply functions that may be necessary for the safety equipment shall be analysed separately.

4.4 Accidents involving severe fuel assembly damages

4.4 (1) For the design of mitigating measures of the internal accident management on level of defence 4c, a spectrum of events shall be postulated that takes into account all relevant phenomena of accidents with severe fuel assembly damages.

In this context, special attention shall be paid to those phenomena that put containment integrity and, if the spent fuel is stored in a fuel pool outside the containment, the integrity of the structure around the fuel pool at risk.

Furthermore, the phenomena that have an effect on the release of radioactive materials and on possible release paths to the environment shall be considered.

4.4 (2) Should no accident management measures have been planned in advance to counteract event sequences or plant conditions or if the accident management measures implemented prove to be ineffective, severe accident management guidelines shall be provided for the emergency response staff. The principle suitability of the severe accident management guidelines to reach the fundamental safety functions shall be demonstrated.

5 Requirements for the safety demonstration

5 (1) The licensee shall be in a position to provide evidence of the safety of the plant.

The safety demonstrations shall be documented in a complete and comprehensible manner. If necessary, they shall be updated.

Note:
Specifications in this respect are presented in Annex 5.

5 (2) Deterministic methods as well as the probabilistic safety analysis shall be applied to demonstrate that the technical safety requirements are fulfilled:
The deterministic methods comprise

a) computational analysis of events or states,

b) measurement or experiment,

c) engineering assessment.

5 (3) The safety demonstration shall be based on:

a) an up-to-date compilation of safety-relevant information about the current condition of the measures and equipment affected as well as

b) a documentation showing that the current condition of the safety-relevant measures and equipment fulfils the applicable requirements.

5 (4) In the computational analysis of event sequences or states,

a) calculation methods shall be used which are validated for the respective scope of application, and

b) any uncertainties associated with the calculation shall be quantified or covered by suitable methods.

5 (5a) To supplement the deterministic safety demonstrations, the balance of the safety-related design shall be verified by probabilistic safety analyses (PSAs).

5 (5b) To supplement the deterministic safety demonstrations, probabilistic safety analyses shall also be done to assess the safety significance

- of modifications of measures, equipment or the operating mode of the plant, as well as
- of findings that have become known from safety-relevant events or phenomena that have occurred and which can be applied to the nuclear power plants in Germany that are referred to in the scope of application of the "Safety Requirements for Nuclear Power Plants"

for which a significant influence on the results of the PSA can be expected.

5 (5c) Compared with the unchanged condition of the plant, modifications of measures, equipment or the operating mode of the plant must not lead to an increase in the average core damage frequency and the average frequency of large and early releases, neither for power operation nor for low-power and shutdown states, considering all plant-internal events as well as all internal and external hazards as well as very rare human-induced external hazards.

5 (6) A measurement or an experiment 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 (7) Engineering assessments may be used for the safety demonstration if assessment criteria exist that are based on scientifically/technically comprehensible fundamentals.

5 (8) The ergonomic design of the conditions for reliable personnel actions according to subsection 3.1 (13) shall be demonstrated by suitable assessment methods.

6 Requirements for the operating rules

6 (1) Written instructions shall exist for the safe operation of a plant, in which the following is specified:

a) A sufficiently complete set of operational limits and conditions (OLCs) which, if observed, ensure that the design, monitoring and operation of the plant fulfil the safety requirements and requirements of the licence. The OLCs shall comprise in particular process-related limits, plant conditions, effectiveness, availability and relevant boundary conditions of safety- relevant plant components to be observed.

The specification of the OLCs shall be based on the plant design, the safety analyses, the licensing conditions and the experience gained from commissioning and operation. The specification of OLCs shall comprise all operational modes.

b) Instructions for the case of deviations from the OLCs.

c) The conditions to be fulfilled to prevent or control events on levels of defence 2 to 4a, events resulting from internal and external hazards and from very rare human induced external hazards. The conditions shall contain all measures necessary for reaching and maintaining a safe plant state.

d) the implemented accident management measures and severe accident management guidelines of the internal accident management. The starting criteria for their application shall be specified. Criteria shall be specified by which it is possible to determine whether long-term compliance with the fundamental safety functions is ensured or a long-term controllable plant state has been reached.

e) The necessary in-service inspections of safety-relevant measures and equipment.

f) The organisational regulations relevant for ensuring safe plant operation (organisational structure and procedural organisation).

g) The minimum requirements for the number and qualification of the personnel and the minimum number of personnel available at the plant for ensuring safe plant operation and control of events on levels of defence 2 to 4; here, initiating events or consequential events resulting from internal or external hazards and from very rare human-induced external hazards as well as personal injury shall also be taken into account.

h) The organisational conditions for the internal accident management.

6 (2) The documents according to subsection 6 (1) shall be provided for the personnel in the main control room and those according to subsection 6 (1) a) to d) for the personnel at the supplementary control room in easily accessible and clear form.

All documents needed for the work of the emergency response staff shall be kept available in the rooms of the emergency response staff.

6 (3) The documents according to subsection 6 (1) shall be kept up to date. For the updating or amendment of the documents, a regulated procedure shall be provided which considers experience feedback and developments in the state of the art of science and technology.

6 (4) Specifications, design codes, material specifications, construction instructions and test codes as well as operating procedures and maintenance standards shall be provided or be in place for all safety-relevant equipment according to their safety relevance.

The test codes shall 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 shall be monitored as part of a quality assurance programme. The results of the quality monitoring and the results of the tests shall be documented. The documents on the design, manufacture, construction and testing as well as on operation and maintenance of the safety-relevant equipment that are necessary for assessing quality shall be kept available until the dismantling of the equipment.

7 Requirements for the documentation

7 (1) The licensee shall have available a systematic, complete, qualified and up-to-date documentation of the state of the nuclear power plant.

Note:
Specifications in this respect are presented in Annex 5.

Annex 1 of the

„Safety Requirements for Nuclear Power Plants“:

Terms and Definitions

22 November 2012

(Words in *italic* are defined in these Terms and Definitions)

A

Abnormal operation

Operational processes that develop in the event of malfunctions of *equipment* or *human error*s (disturbed operating condition) whose occurrence is frequently to be expected over the *service life* of the plant according to operating experience and for which there exist no safety-related reasons against a continuation of operation or the activity (*level of defence* 2). Synonym: *Anticipated operational occurrence.*

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 meeting *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 met. In the event of the occurrence of an accident operation of the plant or of the action cannot 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 monitoring system

Equipment which registers, displays and records information of the plant state 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 involving severe fuel assembly damages

Event sequence with severe fuel assembly damages.

Accident management measure

Special *measure* planned or *equipment* of the *internal 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 treatment

Time period from the *accident* occurrence until reaching a *safe plant state*.

Active loss of function of an instrumentation and control equipment

Malfunction of *instrumentation and control equipment* leading to spontaneous performance of an *instrumentation and control function* without fulfilling the criteria specified for the performance of this function.

Active safety equipment

Equipment of the safety system performing protective actions.

Ageing

Time- and use-dependent changes of function-related features and characteristics of

- technical equipment (structures, systems and components, including electrical systems and instrumentation and control),
- the specification and other reference documents,
- the plant concept and technological procedures,
- of administrative regulations, as well as
- of operating personnel.

Ageing management

The entirety of all *measures* and *equipment* 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 equipment signalling the necessity of a *measure* by optical or acoustic means.

Anticipated operational occurrence (AOO)

An operational process deviating from *normal operation* which is expected to occur at least once during the *service life* of a nuclear power plant but which, in view of appropriate design provisions, does not cause any significant damage to *items important to safety* or lead to *accident* conditions. Synonym for *incident*.

Auxiliary and supply systems

Systems required for the functions of other *systems* or *components*.

Auxiliary power supply

Synonym for station service power supply.

Auxiliary power system

Synonym for station service facility.

Avoidance (to avoid)

The approach of avoiding *events* or event sequences can apply to the case if higher level designed *measures* and *equipment* (on a subsequent *level of defence*) are available for their management in the reliability and effectiveness required. By this means, it has to be ensured that the occurrence of such *events* or event sequences on *level of defence* 3 is not to be expected during the *operating life- time* of the plant, but which have to be postulated in any case.

B

Basis safety

Basis safety means that if the corresponding principles upon *design*, construction, manufacture and *test*ing are adhered to, no far-reaching *failure* of a *component* due to manufacturing-related deficiencies is postulated.

Beyond design basis plant condition

Plant condition after an event sequence with *loss of function* of *safety equipment* such that the necessary effectiveness of *safety function*s to control the course of a *design-basis accident* is no longer given (see also *multiple failure* of *safety equipment*).

Building

Synonym for *structure* or plant *structure*.

By-pass operation

Operation of the water/steam cycle by circumventing the turbine (during the by-pass operation, main steam is directed to the turbine condenser).

C

Cladding failure

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 Requirements 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.

Company 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 company management and all other persons in charge of managerial tasks and the execution level (all persons executing *safety relevant activities*).

Competence of persons

Synonym for qualification of persons.

Component

Part of a *system* defined separately according to structural or functional aspects. Components consist of operating materials. Operating materials consist of *component part*s (see also *structures, systems and components (SSCs*)).

Component part

Part of a piece of *equipment* or the smallest part of a subassembly manufactured from product forms. In construction engineering, a component part is a part of a *building*.

Conservative

The way of proceeding in safety assessments by using well-founded most unfavourable values from a safety point of view under the given circumstances.

Containment penetrations

Constructions 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 the containment and surrounding *building* as well as the *auxiliary systems* for retention and filtering of potential *leakages* from the containment.

Control

An *event* or event sequence is considered to be controlled if the compliance with specified *acceptance targets* and *acceptance criteria* can be demonstrated. Radiologically representative *design basis accidents* are considered to be controlled if the compliance with the radiological *acceptance criteria* is demonstrated.

Controlled plant state

Plant state, following an *anticipated operational occurrence* or *accident,* in which the *fundamental safety function*s are ensured and which can be maintained for a time sufficient to implement pro- visions to reach a safe state.

Such states are characterised by compliance with the *acceptance targets* and *acceptance criteria* and that the relevant *safety variables* have reached sufficiently stationary values.

Sufficiently stationary states are states when the *safety variables* are such stationary or the *safety margin* to the *acceptance criteria* is increasing such steadily that a sufficiently long period of time is available for the analysis and assessment of the plant state enabling the performance of further *measure*s (e.g. *accident treatment*) in case of an unfavourable change of the *safety variables*.

Coolability

State 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 competence

The competence required for planning, performing, controlling and *monitoring* of all activities necessary for the safe operation of a nuclear power plant.

Core component

Component part or *component* of which the reactor core is composed, comprising, in particular, fuel assemblies, control elements, flow restrictors, poisoning and dummy elements, fuel assembly cassettes and cassette fasteners, neutron sources, neutron-absorbing devices of the fuel assemblies and detector assemblies.

Critical nucleate boiling

Boiling condition when film boiling or when dry out of the heating surface starts.

D

Decay heat

The thermal power produced after reactor *shutdown* by radioactive decay or fission (see also *residual heat*).

Defect probability

Probability of the *failure* of the *plant component* concerned, derived on the basis of experiments, in dependence of the respective parameter considered.

Degree of redundancy

Degree of redundancy n + x: n is the number of the minimum required *redundant equipment* where n can vary in different *operational modes* or *plant states*; x is the number of *redundant equipment* to be kept available in addition to n.

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

Event against which a nuclear power plant is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits. Synonym for *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.

Subassembly

Part of a *component* that consists of at least two *component parts*.

Design limit

Acceptance criterion for a parameter considered in the *design*; if this criterion is complied with, a *failure* of the *plant component* concerned needs not be postulated.

Deterministic safety analysis

Analysis of the safety-related state of a plant or a *plant component* for verifying the fulfilment of deterministic safety requirements, consisting of a *system assessment* and a state or *event analysis*.

Disaster control measure

Provision on the basis of the relevant acts of the Laender 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.

Diverse heat sink

Heat sink which is able, independent of the *primary heat sink*, to remove *decay heat* and heat losses from *safety-relevant equipment* arising during operation and *accident*s. Diverse concepts use another *heat sink* than the *primary heat sink* (e.g. air instead of water; well instead of river).

Diversity

Existence of two or more operationally available *equipment* to fulfil the intended function, having different physical and technical *design*s.

E

Emergency control room

Equipment outside the *main control room* from which in case of *loss of function* of the *main control room*, the reactor can be made subcritical, subcriticality can be maintained and heat-removal from the reactor 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 generating units

Equipment that supplies the electrical power in case of loss of function of the station service power supply.

Emergency power supply

Supply of the emergency power consumers from emergency power generating units.

Emergency power supply facility

The combination of specific *emergency power generating units* with all *plant components* required for the supply to the associated consumers.

Emergency power system

Entirety of the *emergency power supply facilities* differing in type of power generation and task.

Emergency equipment

Measures and *equipment* required for the control of an *event* sequence due to a *very rare human induced external hazard* or in the event of the postulated complete unavailability of the *main control room*.

Equipment

Synonym for plant component.

Equipment of the safety system

Equipment of the safety system serving the control of design basis accidents.

Error

(1) Deviation of the specification from the real requirements (specification error).

(2) Deviation of the real quality of a *plant component* from the constructive and manufacturing-related quality 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

Any occurrence unintended by the operator, including operating error, *equipment failure* or other mishap, and deliberate action on the part of others, the consequences or potential consequences of which are not negligible from the point of view of protection or safety.

Event analysis

Analysis element of the *deterministic safety analysis*. Method of *safety demonstration* by which it is demonstrated that sufficiently effective *measure*s and *equipment* are available for the *control* of *events*.

External accident management

All provisions outside the plant for the protection of the population and the environment in case of a threatening, taking place or already concluded *release of radioactive materials*. The external accident management measures are structured into *Disaster Control Measures* and *Radiation Protection Measures.*

External hazard

Impact caused by ambient conditions, natural events or by civilization (according to Annex 3 Section 4.2.3) from outside the plant site. The definition of external hazards used in the "Safety Criteria for Nuclear Power Plants" does not include the *human-induced external hazards*.

F

Failure

Non- or malfunction in case of challenge of active *systems* or loss of *integrity* or *operability* of passive *systems*.

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.

Fire protection means

Structural, plant engineering, operational sand administrative *measures* and *equipment* to prevent the occurrence and propagation of fires, to detect and effectively extinguish fires and to allow the escape and rescue of humans.

Fitness for use

Ability of a *structure* to enable its use as planned under the *impact*s considered in the planning.

Forced reactions under normal operational loads

Reactions of *structural plant components* to operational *impacts*; e.g. forces and moments from temperature, creep, shrinkage and support displacement.

Fuel rod damage

Synonym for cladding failure.

Fundamental safety function

Main *safety function* that comprises different subordinate *safety function*s to be ensured for fulfilment of the respective *acceptance targets* and *acceptance criteria*.

The fundamental *safety function*s are:

a) reactivity control,

b) fuel cooling,

c) confinement of the radioactive materials.

G

Grid connection

Connection between power plant and grid via which the electrical power can be transmitted.

H

Heat sink

Medium (generally a water reservoir or the atmosphere) into which the residual heat can be ultimately transferred.

Heterogeneous boron dilution

Injection of low-borated coolant with consequential significant boron concentration differences in the *primary circuit*.

High-energetic

Pipe or vessel with an operating pressure greater than or equal to 20 bar or an operating temperature greater than or equal to 100°C.

Homogeneous boron dilution

Injection of low-borated coolant without consequential significant boron concentration differences in the *primary circuit*.

Human error

Non-compliance with a requirement during a personnel action.

Human-induced external hazard

Event sequence due to a very rare human-induced *external impact* or due to the postulated complete unavailability of the *main control room*.

I

Impact

Quantities of force and deformation or media with physical, chemical or biological effects or a combi- nation of them acting on *plant components*.

Incident

Event or event sequence which is expected to occur frequently during the *service life* of the plant, for which the plant is designed or for which, with regard to an activity, *measures and equipment* are provided and upon whose occurrence the operation of the plant or the activity can be continued (*level of defence* 2). Synonyms: *abnormal operation,* disturbed operating condition*, anticipated operational occurrence (AOO)*.

Incorporation

Intake of radioactive materials into the human body.

Inherently safe design

Design on the basis of those principles of the laws of nature which by themselves have a safety-directed effect.

Initiating event

An identified *event* that leads to an *anticipated operational occurrence* (AOO) or *accident* and challenges one or more safety functions.

In-service inspection

Test performed at specified intervals.

Inspection

Measure for the identification and assessment of the actual state of *equipment*.

Instrumentation and control

Entirety of the instrumentation and control equipment for the performance of instrumentation and control functions. Instrumentation and control equipment comprise automatic equipment as well as the equipment for process execution by an operator.

Instrumentation and control function

Function for measuring, testing, controlling, *monitoring*, recording and protecting a process or *equipment* (German abbreviation: LEFU).

Instrumentation and control equipment

Equipment for the execution of instrumentation and control functions.

Integrity

State of a *component* or barrier with which the safety-related requirements regarding strength, resistance to fracture and tightness defined for them are fulfilled.

Interlock

Provision by means of which functions of *equipment* which are impermissible under specified operating or *design-basis-accident* conditions are blocked by *instrumentation and control* or process-engineering.

Internal accident management

Measures and equipment on levels of defence 4b and 4c.

Internal hazard

Impact resulting from *events* at the plant site inside or outside *building*s (e.g. fire, plant internal flooding).

Internal flooding

Floodings in *building*s or on the plant site not being directly due to an *external hazard*.

Item important to safety

Synonym for safety-relevant equipment.

L

Leak

Continuous or discontinuous outflow of media from the respective enclosures (e.g. vessels, piping systems, fuel pool) with such an outflow rate that *safety equipment* is actuated.

Leak, large

Leak in the *reactor coolant system* with an outflow area > 0.1 A (A: cross-sectional area of the main coolant line).

Leak, medium

Leak in the *reactor coolant system* with an outflow area ≤ 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 the *accident*.

Leak, small

Leak in the *reactor coolant system* with an outflow area ≤ 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 the *accident*.

Leakage

Continuous or discontinuous outflow of media from the respective enclosures (e.g. vessels, piping systems, fuel pool) with such an outflow rate that *safety equipment* is not actuated.

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: *accident*

Level of defence 4: very rare events (level of defence 4a),

events with *multiple failure of safety equipment* (level of defence 4b), *accident involving severe fuel assembly damages* (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.

Note:
For legal persons and private companies, distinction is to be drawn between

- the responsibility of the respective company as licensee of the nuclear power plant,
- the attending to this responsibility by the company management, i.e. the board members, general managers or another body of this company which is authorised to represent it 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 of process variables

See under limitation system.

Limitation system

Instrumentation and control equipment 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.
- *Limitation of process variables*: Limiting of *process variable* values to maintain initial conditions for *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 *structural plant components.* Here, *impacts* ("load cases") to be postulated or 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 control panel

Equipment outside the *main control room* from which *systems* can be monitored and controlled.

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 function

Loss of the ability of an equipment to fulfil the required function.

Note:
The *event "loss of function"* marks the time point of the transition from correctness to *error.* A loss of function may lead simultaneously to a *failure* but not necessarily, e.g. *equipment* which is not activated can have suffered a loss of function, but it fails only if it will be activated and does not fulfil its function.

Loss-of-coolant accident

Event with loss of reactor coolant from the reactor coolant pressure boundary such that the safety system is actuated.

Low-power and shutdown operation

The *operational mode* that do not serve a targeted nuclear heat production (*operational modes* B to F).

M

Main control room

The central location from which the operation of a nuclear power plant unit is monitored and con- trolled. Parts of the main control room are the control room itself and the adjoining rooms (control room annex).

Main grid

Grid to which the electrical power produced by the nuclear power plant unit can be discharged or from which the nuclear power plant unit can be supplied with electrical power via the *main grid connection*.

Main grid connection

A grid connection via which the electrical power produced by the nuclear power plant unit is discharged to the grid or via which the electrical power can be supplied.

Maintenance

Entirety of the *measures* for keeping and restoring the specified state as well as for the identification and assessment of the real state (including *in-service inspection*). Maintenance is subdivided into *preventive maintenance* with the associated elements *inspection*, *servicing* and *repair*.

Management system

A management system comprises all fixings, regulations and organisational aids which are envisaged within the *company* to plan the tasks relevant for the company's success, to carry out these tasks un- der controlled conditions, to control and to improve the achievement of its goals.

Note:
The management system specified in the Safety Requirements is a process-oriented, integrated management system.

Measure

Action, instruction or organisational activity or organisational process.

Note:
If no action, instruction or organisational activity is referred to, the measure is further specified, e.g.: accident management measure, disaster control measure, etc.

Monitoring

Monitoring is a collective term for all the different types of a controlled determination of physical parameters and includes the comparison with specified values.

Note:
Monitoring is performed e.g. by continuous measurement, discontinuous analysis of samples or calculation of values by correlation of measurement values.

Multiple failure of safety equipment

Event sequence with *loss of function* of *safety equipment* such that sufficient effectiveness of *safety functions* for the control of *accident*s is no longer given.

N

Natural hazards

Impact caused by natural events from outside the plant site.

Near-miss

Potentially safety-relevant *event* which could have been the result of an initiating *event* or an event sequence occurred, but however, did not occurred due to the prevailing *plant condition*s at the time of the *event*.

Non-fixed surface contamination, non-fixed

Contamination of a surface with radioactive materials for which spread of the radioactive materials can be assumed.

Normal operation

The operating conditions and operational processes during correct operable conditions of the *equipment* (undisturbed state), including *in-service inspections* and *maintenance* processes (*level of defence* 1). Operation within specified operational limits and conditions.

O

Operability

Ability of *equipment* to fulfil the envisaged tasks by corresponding mechanical, electrical or other functions.

Operating lifetime

The period during which an authorized facility is used for its intended purpose, until *decommissioning* or *closure*. Synonym: service life.

Operational mode

Operating state of *normal operation* for which specific criteria for availability of system and monitoring functions as well as for process-related conditions are defined.

Operation management

The entirety of all processes and activities that are necessary for the operation of the plant.

Operational monitoring

Controlled recording of operating parameters, including a comparison with specified values. Synonym: process monitoring.

Note:
Monitoring is performed e.g. by continuous measurement, discontinuous analysis of samples or calculation of values by correlation of measured values.

Organisational structure

The organisational structure is the hierarchical framework of an organisation describing the framework conditions for the task management.

P

Passive loss of function of an instrumentation and control equipment

Malfunction of *instrumentation and control equipment* by which an *instrumentation and control function* is not performed when challenged although the criteria specified for the performance of this function are fulfilled.

Passive system part

A *system part* is passive if there will be no change in its positioning in case of challenge (e.g. pipes, vessels, heat exchangers). Self-acting *system parts* (functioning without external power or remote control) shall be considered as passive if the position of the *system part* under consideration (e.g. safety valve or check valve) is not changed in the course of fulfilling its intended function.

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 *structural plant components.*

Plant component

Any structural, mechanical, process-based, electrical or other technical part of a plant. Synonyms are: *equipment*, *system* (see also *structures, systems and components*).

Plant condition

Technical condition of the plant e.g. characterised by the plant's power output, temperature, pressure and coolant level parameters of the *reactor coolant system*.

Plant manager

Staff member who bears the responsibility for the *safe operation* of the entire plant, in particular for the adherence to the requirements of the nuclear legislation and the nuclear licences as well as for the cooperation 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 manual, testing manual, and procedural and working instructions.

Power density oscillation, (global, regional)

Thermal-hydraulic neutron-physically coupled oscillations of the neutron flux:

- global: the neutron flux oscillates in phase over the entire core (also referred to as in-phase or core-wide oscillation);
- 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 *operational mode* of a nuclear power plant in which nuclear heat is produced in a targeted manner (*operational mode* A).

Precautionary measure

Measure or *equipment*, if being in place, the occurrence of an *event* has been demonstrated to be so unlikely that it does not have to be postulated.

Prevention (to prevent)

Events or event sequences for whose *control* there are no higher level designed *measures* or *equipment* on a subsequent *level of defence* shall be prevented. Thus, the progression of *events* and event sequences on *level of defence* 3 to *level of defence* 4 shall be prevented.

Preventive maintenance

*Measure*s for *avoidance* of damage occurrence leading to the unavailability of equipment. Elements of the preventive maintenance *are servicing* and *inspection*.

Primary circuit

System area which comprises the *reactor coolant pressure boundary* in PWR plants. Synonym: primary loop.

Primary coolant

Water which serves the direct cooling of the reactor core in PWR plants.

Primary heat sink

Heat sink to which the *decay heat* as well as the heat losses arising during operation and *accident*s of the *safety-relevant equipment* is ultimately removed.

Probabilistic safety analysis (PSA)

Analysis of the safety- related state of a plant by determination of the frequency of plant hazard states or core damage states or the frequency of the *release of radioactive materials*.

Procedural organisation

The procedural organisation regulates the processes within the framework conditions of the *organisational structure*. The procedural organisation includes all *safety-relevant activities and processes* according to the requirements of the *management system*.

Process variable

A chemical or physical quantity of the process that can be measured directly.

Protective action

The actuation or operation of active *safety equipment* that is needed for the *control* of *event*s.

Protective limitation

See under 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.

Quality

Entirety of features and characteristics of a product or service which refers to their suitability for the fulfilment of given or preconditioned requirements.

R

Radiation protection measure

Provision on the basis of the Precautionary Radiological Protection Act (StrVG) with the objective to keep any radiation exposure of the population and contamination of the environment in case of radiologically significant events as low as achievable taking into account all circumstances.

Reactor coolant

Water which serves the direct cooling of the reactor core in PWR and BWR plants.

Reactor coolant circuit

Synonym for reactor coolant system.

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 serves the direct cooling of the reactor core in PWR and BWR plants. It comprises the *reactor coolant pressure boundary* in PWR and BWR plants, their internals and active *component*s, as well as their support structures.

Reactor protection system

The *equipment* of the reactor protection system is provided for execution of *instrumentation and control functions* of Category A. The reactor protection system is part of the *safety system* which monitors and processes the *process variables* relevant for safety for the *prevention* of unacceptable *impacts* and for the identification of *design-basis accidents* and initiates *protective action*s 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 *equipment* 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 operational available *equipment* than required for the fulfilment of the intended function.

Redundancy-wide impact

Impact resulting from an *internal* or *external hazard* with the potential to cause redundancy-wide *loss of function*s.

Redundant equipment

Equipment which on par with other *equipment* fulfils their functions and, if required, can completely replace one of the other *equipment* or can be replaced by it.

Refuelling

The entirety of all operational activities required to shuffle or replace irradiated fuel assemblies or those that are defective and are to be removed from the core.

Release category

Release categories comprise sequences from accident analyses with similar radionuclide *release*s taking into account further characteristics of the *release* (e.g. nuclide properties, such as, in particular, radiotoxicity and volatility, nuclide composition, time 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 *event*s on *level of defence* 3 or 4.

Reliability analysis

Determination of reliability of *safety-relevant equipment* using probabilistic methods.

Repair

Measures for the restoration of the specified state of *equipment*.

Representative event

Event whose analysis allows an adequate, generically covering *safety demonstration*.

Residual heat

Total of the heat produced by the *decay heat* and the heat stored in the coolant and in *components* or *structural plant components.*

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 or *equipment* for the retention of radioactive materials, e.g. by filtering, water coverage, guided flow by sub-atmospheric pressure, delay lines, vessels, waterproofing of *structure*s, drain pans and other enclosures.

S

Safe operation

The safe operation of a nuclear power plant comprises the nuclear safety, the protection of the environment against ionising radiation, as well as the protection of all persons inside the plant.

Safe plant state

Plant state after occurrence of a *design-basis accident* characterised in that a *controlled plant state* is given and at least the safety related conditions of a comparable *low-power and shutdown operational mode* described in the operating manual are met.

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 factor

Factor to cover uncertainties.

Safety function

Functional combination of *measures* and *equipment* for the fulfilment of safety-related tasks.

Safety margin

Distance between the parameter value permissible according to an *acceptance criteria* and the value in case of which the loss of the required quality has to be assumed.

Safety relevant activities and processes

All activities and processes that may have an influence on the safety of the nuclear power plant.

Safety-relevant equipment (item important to safety)

Equipment required for the safe *shutdown* of the reactor and keeping it in a shutdown state, for *residual-heat removal*, the prevention of uncontrolled criticality as well as necessary precautions against damage and to keep any radiation exposure or contamination of persons, material goods, or the environment as low as achievable, with due regard to the current state of the art in science and technology even below the limits stipulated, at any time during *normal or abnormal operation*, *accident*s, very rare *event*s and in case of *internal and external hazard*s, as well as *human-induced external hazards*.

Safety system

Entirety of all *equipment* that has the task to protect the plant against unacceptable *impact*s 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 or safety-relevant *process variable*.

Segregation

Process-based, electrical and *instrumentation and control* separation of *system parts* to *avoid* mutual disturbance.

Service life

See under operational life time.

Servicing

Measures for conservation of the specified state of *equipment*.

Severe accident management guideline

Generic approach that can be applied if for event sequences or plant states no *accident management measures* have been planned or these *accident management measures* are not effective as planned.

Severe core damage

State of the reactor core with which *coolability* or permanent subcriticality is no longer given.

Severe fuel assembly damage

State of a fuel assembly under which its *coolability* is no longer given.

Shutdown (of the plant)

Controlled load reduction of the plant from *operational modes* A or B to *operational mode* C.

Shutdown reactivity

The reactivity of the reactor transferred to a subcritical state by means of the *shutdown* achieved by the *equipment* provided for this purpose.

Shutdown system

Equipment that is able to transfer the reactor to a subcritical state and maintain it in this state.

Single failure

A *loss of function* that is additionally assumed to occur in *equipment* when actuated 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 *failure*s resulting from a postulated single failure.

A single failure has occurred if a *system part* of the *equipment* does not fulfil its function upon challenge. A *human error* that is possible under operating conditions and which results in a malfunction of the *equipment* is equated with a single failure.

A single failure in a passive *equipment* means the failure of this *equipment*.

Single failure concept

Concept of combining *loss of function* assumptions to be postulated depending on the *level of defence* due to an active or passive *single failure* and unavailability assumptions due to *maintenance* processes.

Software error

Error in software which produces non-specified output data by certain combinations or a certain sequence of input data.

Software failure

Non-fulfilment of functions of the software.

Specified normal operation

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 operational processes

- under correct operable conditions of the *equipment* (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*).

Spiking effect

An effect leading to fission gas release into the coolant during reactor *shutdown* if there are defective fuel pins in the reactor core, due to a decrease of the compressive effect of the cladding onto the fuel.

Spread of radioactive materials

Inadvertent diversion of open radioactive materials.

Station service facility

Entirety of all *plant components* that serve for the electrical power supply of the consumers connected to them and for supplying the *emergency power system*. Synonym: auxiliary power system.

Station service power supply

The electrical power supply of the consumers connected to the *station service facility* and of the systems supplying the *emergency power system* from the main generator, the *main* or *standby grid*. Synonym: *auxiliary power supply*.

Standby grid

Grid from which the nuclear power plant unit can be supplied with electrical power via the *standby grid connection*.

Standby grid connection

A *grid connection* via which at least the electrical energy for *shutdown* of the nuclear power plant can be supplied by keeping the main *heat sink* available.

Startup of the plant

The controlled transfer of the plant to *operational mode* A (*power operation*).

Structure

Synonym for structural element or building (see also structures, systems and components (SSCs)).

Structures, systems and components (SSCs)

A general term encompassing all of the elements (items) of a facility or activity which contribute to protection and safety, except human factors.

Structural element

Synonym for structural plant component.

Structural capability for shutdown of the reactor core

A state of the reactor core in which its *shutdown* by means of the control elements is ensured on the basis of the prevailing geometrical configuration of the reactor core.

Structural plant component

Part of the nuclear power plant assembled from civil construction products (building materials and *component parts*) and connected with the ground. Synonyms: *building, structure, structural element.*

Subsystem

Part of a multiply structured (of similar type) *system* that partially or completely fulfils the function of the *system*.

Supply system

System for the provision of, e.g., electrical power, deionat, auxiliary steam, cooling water, heat, cold, compression air or other technical gases or lubricants.

Support stability

Safety against undue alteration of position and place of a *plant component* (e.g. overturning, dropping, inadmissible slipping).

Surface contamination

Contamination of a surface with radioactive materials comprising activity that is *non-fixed*, fixed and has penetrated through the surface.

System

Synonym for plant component (see also structures, systems and components).

System assessment

Analysis element of the *deterministic safety analysis* for verifying the fulfilment of quality criteria.

Systematic failure

Failure due to a common cause.

Systems outside the primary circuit

Pressure and activity-retaining *systems* and *component*s of safety significance in LWR that are not part of the *reactor coolant pressure boundary*. Safety significance is given if one of the following criteria is given:

a) The *plant component* is necessary for the *control* of *events* on *levels of defence* 3 and 4a with regard to *shutdown*, maintaining long-term subcriticality and direct heat removal.

b) In case of *failure* of the *plant component* large amount of energy is released and the functions of *safety-relevant equipment* are not protected against *impact*s of a postulated *failure* of these *component*s.

c) The failure of the plant component may lead to an event on level of defence 3 or higher, either directly or in a chain of postulated consequential events.

System part

Synonym for *component*.

T

Test

Measure for determining whether the actual state corresponds to the specified state.

Transient

Disequilibrium between power release and power removal, developing in a dynamic way.

U

Uninterrupted emergency power supply

Emergency power supply which after a *loss of function* of the supply from the *station service facility* or from *grid connections* starts to supply from an *emergency power generating unit* (or an electrical power storage) without interruption.

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.

Annex 2 of the

„Safety Requirements for Nuclear Power Plants“:

Events to be considered

22 November 2012

Structure

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 shall be demonstrated by means of computational analyses that the requirements specified in the „Safe- ty Requirements for Nuclear Power Plants" have been met. Especially it shall be demonstrated in accordance with the Annex 5 „Requirements for Safety Demonstration and Documentation" that the safety-related acceptance targets and acceptance criteria applicable on the different levels of defence in depth are achieved and maintained for these events.

Note:
In the event lists, the events are assigned to the applicable fundamental safety functions

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

Those events that are of importance for meeting of radiological safety objectives are marked with (S).

For each fundamental safety function, 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 assembly storage and handling, for the radiological safety objectives in Table 3.3.

1 (2) The fulfilment of the criteria according to subsection 1 (1) is demonstrated on the basis of the operational modes for PWRs and BWRs defined in Tables 4.1 and 4.2.

Where other operational mode definitions are chosen in the plant operating procedures than in the above-mentioned tables, the event lists and the acceptance targets and acceptance criteria assigned to the events shall be adapted accordingly.

1 (3) For defined events whose occurrence can be prevented by special measures and equipment - in the following referred to as precautionary measures - it shall be demonstrated that the requirements for the effectiveness and reliability of these precautionary measures are fulfilled.

For these events, marked with VM in the event lists, computational analysis are required only if it cannot be demonstrated that the specified precautionary measures have been met.

Note:
More detailed and event specific requirements for these precautionary measures are listed in Annex 3 of the „Safety Requirements for Nuclear Power Plants".

2 General Requirements

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 demonstration shall cover the period from event occurrence until reaching a controlled plant state, 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 shall be checked for levels of defence 2 to 4a for all relevant operating conditions.
In this respect, the following working steps shall generally be 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 or adjustment of the lists.

c) As far as appropriate for levels of defence 2 to 4a from a plant-specific point of view, the entirety of the events listed in b) can be attributed to event sequences representative for safety demonstration. The attribution to representative event sequences shall be justified in a detailed and comprehensible manner whereby it shall be demonstrated that the analysed events cover the events not considered.

d) Demonstration of fulfilment of the relevant acceptance criteria and of the general requirements for all events of the plant specific event lists prepared under consideration of steps b) and c).

2 (5) The verifications of fulfilment of the acceptance criteria shall consider the assignment of load levels of the reactor coolant pressure boundary, the systems outside the primary circuit and the containment, presented in Appendix 1 to the events included in the event lists.

3 Nachweisziele und Nachweiskriterien

Tabelle 3.1a: Sicherheitstechnische Nachweisziele und Nachweiskriterien der Sicherheitsebenen 2 bis 4a für die Reaktoranlage und das Schutzziel „Kontrolle der Reaktivität“

Level of defence:	**2**					**3**					**4a**
Operational mode:	**A**	**B**	**C**	**D**	**E**	**A**	**B**	**C**	**D**	**E**	**A**
Fundamental safety function:	**Reactivity control(R)**										
Acceptance targets:	**Power adjustment or reactor shutdown[a)]**					**Reactor shutdown[a)]**					
Acceptance criteria	Also see „Fuel cooling“ and „Confinement of radioactive materials“										
Acceptance target:	**Ensuring subcriticality**										
Acceptance criterion[b)] „Amount of shutdown reactivity":	> 1 %					> 1 %					> 1 %

a) Only operational mode A and with regard to reactor shutdown for BWRs also temporarily in operational mode E during refuelling.

b) Acceptance criteria for the effectiveness of reactor scram (only operational mode A and for BWRs also temporarily in operational mode E during refuelling) and shutdown in the long term (all operational modes). The boundary conditions specified in the “Safety Requirements for Nuclear Power Plants”, subsections 3.2 (6) and 3.2 (7) have to be met.
For refuelling (operational mode E, BWR), failure of fast insertion of the most effective control element has not to be postulated.

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

Level of defence:	**2**					**3**					**4a**
Operational mode:	**A**	**B**	**C**	**D**	**E**	**A**	**B**	**C**	**D**	**E**	**A**
Fundamental safety function:	**Fuel cooling (K)**										
Acceptance targets:	**Unrestricted reuse of the fuel assemblies[a)]**					**Structural capability for shutdown and coolability of the reactor core**					
Acceptance criteria:	- $T_{Fuel} < T_{Melt}$ [b)] - No critical nucleate boiling at cladding tube or meeting of an appropriate temperature-time criterion of the cladding tube			No boiling at the cladding tube		Transient: - Fuel rod integrity[c)] Reactivity accident: - Fuel remains within the cladding tube[d)] LOCA: - Clad temperature < 1200 °C[e)] - Clad oxidation depth < 17 % **Fehler! Textmarke nicht definiert.** - Limitation of cladding tube ballooning[f)]			Fuel rod integrity (maintenance of fuel assembly coverage)[g)]		Transient with postulated scram failure: (operational mode A) Ability of shutdown in the long term and collability

a) The acceptance criteria also to be referred to for ensuring unrestricted reuse within the framework of the design of fuel assemblies and other core internals shall be specified.

b) Fuel melting temperature shall not be reached in the hottest rod under consideration of the radial power distribution in the pellet.

c) No critical nucleate boiling at the fuel rod cladding tubes shall be reached or meeting of an appropriate temperature-time criterion ensuring the integrity of the cladding tube.

d) 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 clad material condition and fuel burn-up.

e) 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 does not occur. Definition of cladding tube oxidation depth: equivalent part of the cladding tube wall consumed by oxidation. Amount of consumed clad- ding 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 shall be demonstrated for the respective cladding tube materials used.

f) Maintenance of a free flow area which ensures sufficient cooling of the fuel rods.

g) As far as accessibility of the containment or the reactor building is required for maintenance of fuel cooling, it shall be 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 fundamental safety function "confinement of radioactive materials"

<table>
<tr><td colspan="2">Level of defence:</td><td colspan="5">2</td><td colspan="5">3</td><td>4a</td></tr>
<tr><td colspan="2">Operational mode:</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</td></tr>
<tr><td colspan="2">Fundamental safety function:</td><td colspan="11">Confinement of radioactive materials (B)</td></tr>
<tr><td colspan="2">Acceptance target</td><td colspan="11">Maintenance of barrier integrity</td></tr>
<tr><td rowspan="7">Acceptance criteria</td><td></td><td colspan="11">See „Fuel cooling“</td></tr>
<tr><td>Fuel rod cladding tube</td><td>PCI[a)]</td><td colspan="4">-</td><td colspan="3">LOCA < 0,1 F:
Fuel rod damage extent < 1 %
LOCA > 0,1 F:
Fuel rod damage extent < 10 %</td><td>-</td><td>-</td></tr>
<tr><td>Reactor coolant pressure boundary</td><td colspan="5">See Appendix 1</td><td colspan="4">See Appendix 1</td><td>See Appendix 1</td></tr>
<tr><td>External systems [b)]</td><td colspan="5">See Appendix 1</td><td colspan="4">See Appendix 1</td><td>See Appendix 1</td></tr>
<tr><td rowspan="3">Containment</td><td colspan="3">Pressure increase in the containment < response criteria reactor protection system</td><td rowspan="2">-</td><td colspan="3">$P_{cont.} \leq P_{cont.}\text{-}A$[c)]</td><td rowspan="2">-</td><td>$P_{cont.} \leq P_{cont.}\text{-}A$</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 < 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 Appendix 1</td><td colspan="4">See Appendix 1</td><td>See Appendix 1</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) External systems do not represent one of the three barriers stated in the barrier concept. The safety-related relevance of the maintenance of the external systems integrity is primarily based on the maintenance of the heat removal from the reactor core. However, as in the case of the reactor coolant pressure boundary, too, external systems are listed in Table 3.1c as reference is made to the load levels of the Annex 1.

c) For the determination of the differential pressures inside the containment see Annex 5 of the "Safety Requirements for Nuclear Power Plants" ("Requirements for Safety Demonstration and Documentation"), Appendix 2.

Level of defence:	2					3					4a
Operational mode:	A	B	C	D	E	A	B	C	D	E	A
Fundamental safety function:	Confinement of radioactive materials (B)										
Acceptance target:	Maintenance of retention function of equipment										
Acceptance criteria:	No event-specific analysis demanded, otherwise see under “Achievement of the radiological safety objectives”					see under “Achievement of the radiological safety objectives”					-

Table 3.2: Safety-related acceptance targets and criteria of level of defence 2 to 4a for fuel assembly storage and handling

Level of defence:	**2**	**3**
Operational mode:	**A – F**	**A – F**
Fundamental safety function:	**Reactivity control (R)**	
Acceptance target:	Ensuring subcriticality	
Acceptance criterion: **Neutron multiplication factor k_{eff}:**	< 0,95	< 0,95 [a)]
Fundamental safety function:	**Fuel cooling (K)** [c)]	
Acceptance targets:	Limitation of the spent fuel pool water temperatures to values which ensure accessibility of the pool area with customary measures	Limitation of the spent fuel pool water temperatures to values below the design temperature of the pool for ensuring its integrity [b)]
	Sufficient water coverage for ensuring the required inlet condition for the pool pumps	Sufficient water coverage for ensuring fuel assembly cooling
Acceptance criteria:	Maintenance of specified spent fuel pool water temperatures	
Fundamental safety function:	**Confinement of radioactive materials (B)** [c)]	
Acceptance targets:	See under “Fuel cooling“	
	Maintenance of the retention function of buildings and systems:	
Acceptance criteria:	No event-specific analysis demanded, otherwise see under “Achievement of the radiological safety objectives”	see under “Achievement of the radiological safety objectives”

a) For special events (see event list Table 5.3): < 0.98.

b) As far as accessibility of the containment or the spent fuel pool area is required for maintenance of fuel cooling, it shall be demonstrated that the conditions for accessibility are fulfilled.

c) Acceptance targets only applicable to wet storage and handling processes.

Table 3.3: Radiological safety objectives of levels of defence 2 to 4a for the reactor plant and fuel assembly storage and handling

Level of defence:	**2**						**3**						**4a**
Operational mode:	**A**	**B**	**C**	**D**	**E**	**F**	**A**	**B**	**C**	**D**	**E**	**F**	**A**
	Achievement of the radiological safety objectives (S)												
Compliance with the specifications of the Radiation Protection Ordinance (StrlSchV):	Plant-specific license values for the disposal of radioactive material within air or water in compliance with the §47 StrlSchV						Compliance with the accident planning levels according to §49 StrlSchV						-

4 Definitions and delineations of the operational modes for PWRs and BWRs

Table 4.1: Definition of the operational modes for PWRs

Mode	Description	System conditions (normal operation)	K_{eff} [1)]
A	Nuclear power and start-up operation	Plant during power operation or ready to start power operation	≥ 0,99
B	Hot subcritical	Residual-heat removal via residual heat removal system not possible	< 0,99
C	Cold subcritical primary system pressure-tight closed	Residual heat removal via residual heat removal system Primary system pressure-tight closed	< 0,99 [2)]
D	Cold subcritical primary system not pressure-tight closed	Primary system not pressure-tight closed and refuelling cavity not completely flooded	< 0,95 [2)]
E	Refuelling	Refuelling cavity completely flooded	< 0,95 [2)]
F	Fuel assembly storage	All fuel assemblies in the spent fuel pool separated from the refuelling cavity Fuel assembly cooling via spent fuel pool cooling system	< 0,95

Notes:

1) Further requirements to k_{eff} values required in accordance with the operational instructions may result from the safety demonstration for the control of events on level of defence 2 and 3 (safety margin for event sequences to be controlled).

2) In case of a control-element-free reactor core

Table 4.2: Definition of the operational modes for BWRs

Mode	Description	System conditions (normal operation)	K_{eff}[1)]
A	Nuclear power and start-up operation	Plant during power operation or during start-up operation from the start of control element withdrawal	≥ 0,99
B[2)]	Hot subcritical	Control elements completely inserted and residual-heat removal via residual-heat removal system not possible	< 0,99
C	Cold subcritical primary system pressure-tight closed	Residual-heat removal via residual-heat removal system Reactor coolant circuit pressure-tight closed	< 0,99[3)]
D	Cold subcritical primary system not pressure-tight closed	Reactor coolant circuit not pressure-tight closed and refuelling cavity not completely flooded	< 0,99
E	Refuelling	Refuelling cavity completely flooded Fuel assemblies in the reactor and in the spent fuel pool	< 0,99 for reactor[4)] < 0,95 for spent fuel pool
F[5)]	Fuel assembly storage	All fuel assemblies in the spent fuel pool separated from the refuelling cavity Fuel assembly cooling via spent fuel pool cooling system	< 0,95

Note:

1) Further requirements to k_{eff} values required in accordance with the operational instructions may result from the safety demonstration for the control of events on level of defence 2 and 3 (safety margin for event sequences to be controlled).

2) During start-up operation of the BWR from cold condition, direct transition from Phase C to Phase A due to heating up caused by control element insertion occurs.

3) During zero-power tests, withdrawal of a certain number of control elements is required to reach a critical state.

4) Not during function and subcriticality tests or shutdown safety test; thereby no more than 2 control elements not inserted.

5) For a BWR plant, operational mode F is only given in special cases (e.g. for reactor pressure vessel pressure test).

5 Event lists

Note:
Explanations on the event lists:

For both power operation and low-power and shutdown operation modes of PWRs and BWRs, the event lists cover levels of defence 2 to 4a; for the spent fuel pool (PWRs and BWRs), the event lists cover levels of defence 2 to 3 according to the „Safety Requirements for Nuclear Power Plants“. For levels of defence 2 to 4a, there are comprehensive spectra of events. For plant-specific analyses, the listing may be condensed to representative events, if documented justification is provided according to subsection 2 (4), or may be extended or modified according to the licensing situation. The approach on level of defence 4b and 4 c is presented in special regulations.

Events to be considered due to internal and external hazards as well as in case of very rare human-induced external hazards are listed in Annex 3 of the „Safety Requirements for Nu- clear Power Plants“.

Events due to disruptive actions or other interference 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 operating condition or operational mode.

For PWRs, the event categories are:

- Change of secondary-side heat removal,
- Secondary-side heat removal – accidents involving leaks,
- 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,
- Loss of coolant within the containment,
- Loss of coolant outside the containment,
- Release of radioactive material from nuclear auxiliary systems,
- Loss of energy supply,
- Events due to an internal hazard and
- Anticipated transient without scram (ATWS).

For BWRs, the event categories are:

- Main-steam- or feedwater-side change of heat removal,
- Change of flow rate in the reactor coolant system,
- 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,
- Release of radioactive material from nuclear auxiliary systems,
- Loss of energy supply,
- Events due to an internal hazard and
- Anticipated transient without scram (ATWS).

For the fuel storage, the following event categories are applicable to both PWRs and BWRs:

- Reduced heat removal from the spent fuel pool,
- Loss of coolant from the spent fuel pool,
- Loss of energy supply,

- Reactivity changes during fuel storage and
- Events during handling and storage of fuel assemblies.

The columns of the event lists begin with the numbering (Xy-x; X represents D (for PWR, in German DWR), S (for BWR, in German SWR) or B (for the spent fuel pool), y = level of de- fence 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 fundamental safety functions concerned, the relevant operational modes, additional comments on the acceptance criteria and, where appropriate, details on additional boundary conditions and event-specific notes.

The letters in the column “fundamental safety functions concerned” indicate for each event those fundamental safety functions for which effectiveness of the measures and equipment shall be demonstrated. The acceptance criteria generally applicable to the different fundamental safety functions are - for both power operation (operational mode A) and low power and shutdown operation (operational modes B-F) of PWRs and BWRs as well as for the spent fuel pool – included in Section 3 which specifies the acceptance criteria for the levels of defence and operational modes.

Events for which there is the possibility to demonstrate effectiveness and reliability of pre- cautionary measures instead of performing deterministic event analyses in order to show the control of these events are marked with VM.

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

In the column operational modes, those modes 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 and breaks, however, are events of level of defence 3. Here, the flow rate is so high that the safety system is activated automatically.

For leaks and breaks, the analysed maximum flow 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 Appendix 2.

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

No.	PWR events	Fundamental safety functions concerned	Operational mode	Additional comments, boundary conditions and notes
Level of defence 2				
Change of the secondary-side heat removal				
D2-01	Malfunction in the main steam system or in the feedwater supply system which leads to an unplanned temperature/pressure decrease in the steam generator.	R	A	Note: • e.g. control fault, loss of high-pressure feedwater heater, inadvertent actuation of a main steam turbine bypass, inadvertent actuation of auxiliary steam supply.
D2-02	Malfunction in the main steam system or in the feedwater supply system which leads to an unplanned temperature/pressure in- crease in the steam generator.	K	A-B	Note: • e.g. turbine control faults, partially inadvertent closure of main steam isolation valves.
D2-03	Inadvertent closure of valves leading to significant changes in main steam or feed- water flow rate.	K, B	A-B	
D2-04	Turbine trip with opening of the turbine bypass.	R, K, B	A	
D2-05	Turbine trip with delayed loss of the bypass station or without opening of the turbine bypass.	R, K, B	A	
D2-06	Loss of main heat sink	R, K, B	A-B	
D2-07	Load rejection to station service power	R, K, B	A	Additional boundary condition: • With and without switching to off-site power supply.
D2-08	Loss of main feedwater pump without switch-on of standby pump	R, K	A	

No.	PWR events	Fundamental safety functions concerned	Operational mode	Additional comments, boundary conditions and notes
D2-09	Loss of all main feedwater pumps, in operation, with and without switch-on of standby pump	R, K	A	
Change of flow rate in the primary circuit				
D2-10	Loss of a main coolant pump	R, K	A-B	
D2-11	Loss of all main coolant pumps	R, K, B	A-B	
Pressure change in the primary circuit				
D2-12	Pressure drop due to inadvertent pressuriser spraying actuation or inadvertent valve opening	K	A-B	
D2-13	Pressure increase due to inadvertent switch-on of pressuriser heater	B	A-C	
Increase of reactor coolant inventory				
D2-14	Inadvertent injection or reduction of extraction rates by operational systems or safety systems	K, B	A-C	
Decrease of reactor coolant inventory				
D2-15	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 operational modes B and C shall be considered.
D2-16	Malfunction in the volumetric control system leading to a reduction of the coolant inventory	K	A-C	
D2-17	Level drop during mid-loop operation	K	C-D	Note: • Successful prevention of loss of residual-heat removal pumps due to level drop shall be verified.

No.	PWR events	Fundamental safety functions concerned	Operational mode	Additional comments, boundary conditions and notes
D2-18	Leakages at pressuriser (in steam region)	K	A-B	Note: • Without automatic actuation of the safety system.
Loss of residual heat removal				
D2-19	Loss of one train, in operation, of the residual heat removal system	K, B	C-E	Additional boundary condition: • Single failure shall not be postulated.
D2-20	Loss of all residual heat removal trains due to faulty signals (short-term)	K, B	C-E	Additional boundary condition: • The operating limits for the residual heat removal system will not be exceeded.
Change of reactivity and power distribution				
D2-21	Malfunction in the reactor power control system	R, K	A	
D2-22	Inadvertent withdrawal of the most effective control element or the most effective control element group without loss of function of limitation systems	R, K	A-B	
D2-23	Inadvertent fall in or insertion of one or more control elements	R, K	A	
D2-24	Inadvertent injection from a system carrying deionized water or low-borated coolant (external boron dilution; homogeneous and heterogeneous)	R	A-E	

No.	PWR events	Fundamental safety functions concerned	Operational mode	Additional comments, boundary conditions and notes
D2-25	Most unfavourable wrong loading of a most reactive fuel assembly	R, K	E, A	Additional boundary condition: • Reactor startup with wrong loaded fuel assembly shall be analysed regarding fundamental safety function K in operational mode A. Comment: • Fundamental safety function R (subcriticality) in operational mode E, • Fundamental safety function K in operational mode A Optionally, it may be shown regarding fundamental safety function K that reactor startup with the wrong loaded fuel assembly is excluded by corresponding precautionary measures.
D2-26	Non-compliance with the switch-on conditions when switching on a main coolant pump after 3-Loop-operation	R, K	A	
D2-27	Cold water injection into the reactor coolant system from a connected system (e.g. by- pass of the recuperative heat exchanger of the volumetric control system)	R	A-B	
Loss of energy supply				
D2-28	Loss of offsite power equal or less than 10 hours	R, K, B	A-E	Additional boundary condition: • Switch back to main or standby grid shall also be analysed.

No.	PWR events	Fundamental safety functions concerned	Operational mode	Additional comments, boundary conditions and notes
Level of defence 3				
Change of the secondary-side heat removal				
D3-01	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.	R, B, S	A-C	Additional boundary condition: • Operationally permissible steam generator tube defects shall be 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 mode B and in mode A at low power. Inadvertent opening in mode B more probable than in mode A due to performance of tests.
D3-02	Major 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, B, S	A-B	Additional boundary condition: • Operationally permissible steam generator tube defects shall be considered. • Cases to be considered: e.g. inadvertent closure of two up to all main steam isolation valves.
D3-03	Loss of feedwater supply	K	A-B	Note: • This includes loss of feedwater supply and loss of equipment used during startup and shutdown (startup and shutdown system or emergency feedwater system during operating conditions).
D3-04	Malfunction in the feedwater supply, leading to an impermissible coolant level in the steam generator.	K	A-B	

No.	PWR events	Fundamental safety functions concerned	Operational mode	Additional comments, boundary conditions and notes
Secondary-side heat removal – accidents involving leaks				
D3-05	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 Appendix 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 shall be considered.
D3-06	Leak/break in main steam or feedwater system or other high-energy piping systems in the annulus and in the valve compartments	R, K, B, S VM	A-B	Additional boundary condition: • Operationally permissible steam generator tube defects shall be considered for leak/break in the main steam and feedwater system. • Details on the leak and break assumptions and on safety demonstrations are included in Appendix 2. • VM option is only permissible for piping area between the end of guard pipes in the annulus and the main steam isolation valve. See also “Safety Requirements for Nuclear Power Plants” Annex 3, Section 3.2.4. Special consideration of: • the integrity of the containment, • the 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.
D3-07	Leak/break in main steam or feedwater system behind the main steam isolation valve and in front of the feedwater isolation valve	R, K, B, S	A-C	Additional boundary condition: • Operationally permissible steam generator tube defects shall be considered for leak/break of the main steam line. • Details on the leak and break assumptions and on the safety demonstration are included in Appendix 2.

No.	PWR events	Fundamental safety functions concerned	Operational mode	Additional comments, boundary conditions and notes
D3-08	Main steam line rupture after first isolation with 2A break of a steam generator tube	R, K, B, S	A-B	Additional boundary condition: • Details on the leak and break assumptions and on safety demonstrations are included in Appendix 2. • The random break of a steam generator tube can be considered as a single failure.
D3-09	Inadvertent opening of a main steam safety valve with 2A break of a steam generator tube	R, K, B, S	A-B	Additional boundary condition: • The random break of a steam generator tube can be considered as a single failure.
Change of flow rate in the primary circuit				
D3-10	Break of a main coolant pump shaft	R, K	A	Additional boundary condition: • Immediate blocking of the impeller shall also be considered.
Increase of reactor coolant inventory				
D3-11	Inadvertent injection by operational systems or by safety equipment in case of ineffectiveness of limitation measures provided	K, B	A-C	
Decrease of reactor coolant inventory				
D3-12	Inadvertent level drop during mid-loop operation with consequential loss of residual heat removal pumps	R, K, B	C-D	Comment: • Fundamental safety function R affected due to reflux condenser mode in mode C. • Fundamental safety function B is relevant for operational mode C (primary circuit closed).
Loss of residual-heat removal				
D3-13	Loss of one train, in operation, of the residual heat removal system	K, B	C-E	Additional boundary condition: • In contrast to event D2-20, here with consideration of the single failure.
D3-14	Loss of all residual heat removal trains due to faulty signals	K, B	C-E	Additional boundary condition: • The analysis shall consider the ineffectiveness of personnel actions required in the short term (see event D2-21).

No.	PWR events	Fundamental safety functions concerned	Operational mode	Additional comments, boundary conditions and notes
Change of reactivity and power distribution				
D3-15	Inadvertent withdrawal of the most effective control element or the most effective control element group with loss of function of limitation systems	R, K	A-B	
D3-16	Ejection of the most effective control element	R, K	A-B	
D3-17	Wrong loading of the reactor core with more than one fuel assembly	R VM	E	Comment: • Alternatively to the demonstration of subcriticality, precautionary measures can be taken, so that wrong loading of the reactor core with more than one fuel assembly is prevented.
D3-18	Fall of a fuel assembly onto the reactor core	R	E	Additional boundary condition: • Demonstration of subcriticality with fuel assembly lying on the core

No.	PWR events	Fundamental safety functions concerned	Operational mode	Additional comments, boundary conditions and notes
D3-19	Inadvertent injection from a system carrying deionized water or low-borated coolant with loss of function of the limitation system or preceding measures (external boron dilution; homogeneous and heterogeneous).	R, K VM	A-E	Additional boundary condition: The following shall be considered: • All possibilities and amounts for injection of deionized water, • Operator failure, e.g. inadvertent filling of tanks, • Input from connected systems via heat exchanger tubes, seals or valve seat leakages, • Inadvertent injection into the primary circuit, • Feedwater injection during shutdown under loss of offsite power conditions after steam generator tube rupture. It shall be demonstrated that reactivity changes due to injection of deionized 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. Inadmissible entry of deionized water from external sources shall be prevented by measures and equipment.

No.	PWR events	Fundamental safety functions concerned	Operational mode	Additional comments, boundary conditions and notes
D3-20	Formation of low-borated areas in the primary circuit (internal boron dilution)	R, K VM	A-C	Additional boundary conditions: Potential sources of formation of low-borated areas shall be investigated. Causes may be, e.g.: • Reflux condenser operation after small break LOCA, taking into account the inserted control elements (under consideration of the „Safety Requirements for Nuclear Power Plants“ subsection 3.2 (7)) and the time-dependent xenon concentration, and, • Shutting down the reactor 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 shall be demonstrated that reactivity changes due to injection of deionized water into the reactor coolant system remains limited to such values where for an initially subcritical reactor the amount of shutdown reactivity required according to Table 3.1a is complied with.
D3-21	Subcooling transients due to leak or break of main steam or feedwater line	R, K	A-B	Specification of the acceptance criteria: • Recriticality shall only be permissible for leaks in the main steam line if fast cool-down of the primary circuit is possible and provided that the criteria for cooling of the fuel assemblies are fulfilled. • Leak size leading to the highest subcooling shall be identified.

No.	PWR events	Fundamental safety functions concerned	Operational mode	Additional comments, boundary conditions and notes
Loss of coolant within the containment				
D3-22	Small break within the containment	R, K, B, S	A-B	Additional boundary condition: • Reflux condenser mode shall be considered (see D3-20). • Details on the leak and break assumptions and on safety demonstrations are included in Appendix 2. • Further specifications see Annex 5, Appendix 1, A1 (2). Note: • Characteristic feature: Secondary-side heat removal necessary for the control of that accident.
D3-23	Medium break within the containment (leak cross section ≤ 0.1F)	R, K, B, S	A-B	Additional boundary condition: • For details on the leak and break assumptions and on the required safety demonstrations, see Appendix 2. • Further specifications see Annex 5, Appendix 1, A1 (2). Note: • Characteristic feature of the medium break: Heat removal via leak sufficient => secondary-side heat removal for control of the accident not generally necessary.

No.	PWR events	Fundamental safety functions concerned	Operational mode	Additional comments, boundary conditions and notes
D3-24	Large break within the containment (leak cross section > 0.1F)	R, K, B, S	A-B	Additional boundary condition: • Details on the leak and break assumptions and on safety demonstrations are included in Appendix 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 the accident. • Further specifications see Annex 5, Appendix 1, A1 (2). 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.
D3-25	Leak at the pressuriser in the steam region without reaching the containment pressure criterion	R, K, B, S	A-B	Note: • With automatic activation of the safety system.
D3-26	Leak at the connecting nozzle of the main coolant line on reactor pressure vessel	K	A-B	Additional boundary condition: • It shall be demonstrated that impermissible impacts on the structure of the reactor cavity and the anchoring of the reactor pressure vessel are prevented. • Further, the consequences of the event regarding sufficient coverage of sump suction lines with coolant in case of considered dead end volumes within the reactor cavity shall be considered.
D3-27	„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 cm^2 is design-relevant for the flow-off conditions at the biological shield and the maintenance of its safety function.

No.	PWR events	Fundamental safety functions concerned	Operational mode	Additional comments, boundary conditions and notes
D3-28	Leak in reactor pressure vessel closure head area	R, K, B, S	A-B	Additional boundary condition: • For the control of the event it shall be 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, i.e. a sufficiently dimensioned connection between refuelling cavity and the sump in operational modes A and B shall be ensured. • Details on the leak and break assumptions and on safety demonstrations are included in Appendix 2.
D3-29	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. man- holes). • This analysis shall consider that at the time of onset of the accident a fuel assembly is being transported in the most unfavourable position. Here, the acceptance criterion is maintenance of cladding tube integrity. • Requirement for emergency core cooling effectiveness; limited availability of safety equipment (e.g. reactor protection) shall be considered.
D3-30	Inadvertent opening and/or stuck open of a pressuriser safety valve or pressuriser relief valve, e.g. during functional tests	K, B	A-C	Additional boundary condition: • The limited availability of safety equipment (e.g. reactor protec-tion) shall be considered.
D3-31	Failure of a steam generator tube (larger than operationally permissible leakages and up to max. 2 A)	K, B, S	A-B	Additional boundary condition: • The event shall be 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-loop operation.

No.	PWR events	Fundamental safety functions concerned	Operational mode	Additional comments, boundary conditions and notes
Loss of coolant outside the containment				
D3-32	Leak in residual heat removal system in annulus during residual heat removal operation	K, B, S VM	C-E	Additional boundary condition: • Details on leak and break assumptions and on safety demonstration are included in Appendix 2. Comment: • There is the option of demonstrating that in case of leaks in the residual-heat removal system in the annulus, safety-relevant flood events are prevented due to realised precautionary measures in the respective operational modes.
D3-33	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.
D3-34	Loss of coolant from the containment via systems connected to the reactor coolant pressure boundary	K, B, S	A-C	
D3-35	Leaks in systems with flooding potential in the annulus	K, B, S, VM	A-E	Additional boundary condition: • All relevant sources from leaks and tank failure of systems and equipment in the annulus, in particular the containment sump suction line, shall be considered. • Further, the boundary conditions within during maintenance measures shall be considered (see Annex 3, Section 3.2.2).
Release of radioactive material from nuclear auxiliary systems				
D3-36	Leak in the volumetric control system out-side the containment	S	A-F	Additional boundary condition: • Details on the leak and break assumptions and on safety demonstrations are included in Appendix 2. • Spiking effect shall be considered.
D3-37	Leak in an instrumentation line carrying primary coolant in the annulus	S	A-F	
D3-38	Leak/break in a pipe or break of a filter in the off-gas or gas treatment system	S	A-F	

No.	PWR events	Fundamental safety functions concerned	Operational mode	Additional comments, boundary conditions and notes
D3-39	Leak in tank with active medium	S	A-F	Additional boundary condition: • The tank with the largest radiological hazard potential shall be identified. • The analysis shall consider tank failure resulting from earth-quake.
Loss of energy supply				
D3-40	Loss of offsite power for more than 10 hours	R, K, B, S	A-E	Additional boundary condition: • The shutdown under loss of offsite power conditions shall also be analysed. • Operationally permissible steam generator tube leakages shall be considered.
Events resulting from an internal hazard				
D3-41	Potential activity releases resulting from internal fires (including filter fire) or explosions	S, VM	A-F	Additional boundary condition: • Analyses on fires and explosions at components or systems areas with high activity release potential shall be performed. Comment: • For the compliance with the fundamental safety function S, there is the option of demonstrating that, due to existing fire and explosion protection means, radiologically relevant impacts are excluded.
D3-42	Break of a control element nozzle with control element ejection	R, K, B, S	A-B	Additional boundary condition: • In addition to the control of the resulting leak it shall be demonstrated that the ejection of the control element does not lead to an impermissible damage. Further, it shall be demonstrated that no consequential damages of neighbouring drives occur that impair the functional safety of other control elements. If consequential damage cannot be prevented, it shall be demonstrated that the acceptance criteria are fulfilled anyhow.

No.	PWR events	Fundamental safety functions concerned	Operational mode	Additional comments, boundary conditions and notes
Level of defence 4				
Level of defence 4a				
Anticipated transient without scram (ATWS)				
D4a-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	
D4a-02	Loss of main heat sink with unavailable auxiliary power supply	R, K, B	A	
D4a-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	
D4a-04	Total loss of main feedwater supply	R, K, B	A	
D4a-05	Maximum reduction of the coolant flow rate	R, K, B	A	
D4a-06	Maximum reactivity insertion by withdrawal of control elements or control element groups starting from full power and from „hot subcriticality“	R, K, B	A	
D4a-07	Depressurisation due to inadvertent opening of a pressuriser safety valve	R, K, B	A	
D4a-08	Maximum reduction of the reactor inlet temperature caused by a fault in an active component of the feedwater supply.	R, K, B	A	

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

No.	BWR events	Fundamental safety functions concerned	Operational mode	Additionally comments, boundary conditions and notes
Level of defence 2				
Main-steam- or feedwater-side change of heat removal				
S2-01	Malfunctions in the main steam system or in the feedwater supply system leading to an unplanned temperature or pressure decrease in the reactor coolant system.	R, K	A-B	Additional boundary condition: • Impact on neutron-physical-thermal-hydraulic stability of the core shall be considered. Note: • e.g. control fault, loss of high-pressure preheater, inadvertent actuation of auxiliary steam supply or one of the safety and relief valves.
S2-02	Malfunction in the main steam system or in the feedwater supply system leading to an unplanned temperature/pressure increase in the reactor coolant system.	R, K, B	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.
S2-03	Turbine trip with opening of the turbine by-pass	R, K, B	A	
S2-04	Turbine trip with delayed loss of the bypass or without opening of the turbine bypass station	R, K, B	A	
S2-05	Loss of main heat sink	R, K, B	A-B	
S2-06	Load rejection to auxiliary power	R, K B	A	Additional boundary condition: • With and without switch back to main and standby off-site power supply.
S2-07	Loss of one feedwater pump without switch-on of the standby pump	R, K	A-B	
S2-08	Loss of all feedwater pumps with and without switch-on of the standby pump	R, K	A-B	

No.	BWR events	Fundamental safety functions concerned	Operational mode	Additionally comments, boundary conditions and notes
Change of flow rate in the primary circuit				
S2-09	Loss of individual/several/all reactor recirculation pumps	R, K	A-B	Additional boundary condition: • Impact on neutron-physical-thermal-hydraulic stability of the core shall be considered.
Increase of reactor coolant inventory				
S2-10	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.
S2-11	Inadvertent injection with one train of the emergency core cooling systems	-	D	Additional boundary condition: • Relevant for procedures. • Only relevant in operational mode D due to overfilling of reactor pressure vessel in case of not installed reactor cavity seal liner. Specification of the acceptance criteria: • Ensuring of coolant inventory in the long-term.
Decrease of reactor coolant inventory				
S2-12	Leakage from reactor pressure vessel bot- tom resulting from maintenance	K	E	Note: • Relevant for procedures. • Limit: Leakage can be overfed by operational systems.
Loss of residual heat removal				
S2-13	Loss of one train, in operation, of the residual heat removal system	K, B	C-E	Additional boundary condition: • Single failure shall not be postulated.
S2-14	Shutdown of all residual heat removal trains due to pressure increase or coolant level decrease	K, B	C-D	
Change of reactivity and power distribution				
S2-15	Withdrawal of the most effective control element or of the most effective control element group	R, K	A, C, E	

No.	BWR events	Fundamental safety functions concerned	Operational mode	Additionally comments, boundary conditions and notes
S2-16	Inadvertent fast insertion or inadvertent insertion of a control element	R, K	A	
S2-17	Inadvertent insertion of all control elements at high power	R, K	A	
S2-18	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 neutron-physical-thermal-hydraulic stability of the core shall be considered.
S2-19	Malfunction in the reactor power control	R, K	A	
S2-20	Most unfavourable wrong loading of a most reactive fuel assembly	R, K	E, A	Additional boundary condition: • Reactor startup with wrong loaded fuel assembly shall be analysed regarding fundamental safety function K in operational mode A. Comment: • Fundamental safety function R (subcriticality) in operational mode E. • Fundamental safety function K in operational mode A. Optionally, it may be shown regarding fundamental safety function K that reactor startup with the wrong loaded fuel assembly is excluded by corresponding precautionary measures.
S2-21	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.
Loss of energy supply				
S2-22	Loss of offsite power equal or less than 10 hours	R, K, B	A-E	Additional boundary condition: • Switch back to main or standby grid shall also be analysed.

No.	BWR events	Fundamental safety functions concerned	Operational mode	Additionally comments, boundary conditions and notes
Level of defence 3				
Main-steam- or feedwater-side change of the removal				
S3-01	Major malfunction in the main steam system or in the feedwater supply system leading to temperature or pressure decrease in the reactor coolant system.	R, K	A-B	Note: • Contrary to event S2-01, here, simultaneous inadvertent opening of several valves e.g. inadvertent complete opening of main steam bypass valve, inadvertent opening of safety and relief valves.
S3-02	Major malfunction in the main steam system or in the feedwater supply system leading to temperature or pressure increase in the reactor coolant system.	R, K, B, S	A-B	Note: • e.g. inadvertent closure of all main steam isolation valves
S3-03	Loss of all feedwater pumps without switch- on of the standby pump	R, K	A	Additional boundary condition: • Contrary to event S2-08, here, consideration of the single failure concept.
Increase of reactor coolant inventory				
S3-04	Functional failure with increase of coolant level in the reactor pressure vessel or inadvertent injection by operational systems or safety systems	R, B	A-C	Additional boundary condition: • Contrary to event S2-10, here, consideration of the single failure concept.
Loss of residual-heat removal				
S3-05	Loss of one train, in operation, of the residual heat removal	K, B	C-E	Additional boundary condition: • Contrary to event S2-13 here, consideration of the single failure concept.
S3-06	Shutdown of all residual heat removal trains due to pressure increase or coolant level decrease	K, B	C-D	Additional boundary condition: • Contrary to event S2-14 here, consideration of the single failure concept.

No.	BWR events	Fundamental safety functions concerned	Operational mode	Additionally comments, boundary conditions and notes
Change of reactivity and power distribution				
S3-07	Inadvertent reactivity insertion due to loss of high-pressure preheater and unavailability of limitation systems	R, K	A	
S3-08	Withdrawal of the most effective control element or control element group with loss of limitation systems	R, K, VM	A, B, D	Comment: • Alternatively to the analysis, for mode D, it can be ensured by appropriate precautions that withdrawal of the most effective control element or control element group is prevented.
S3-09	Ejection of the most effective control element	R, K	A	
S3-10	Drop out of the most effective control element	R, K	A	Additional boundary condition: • Drop out over the length of a latch distance.
S3-11	Drop of a fuel assembly into the just not yet critical reactor core (BWR)	R, K, VM	E	Comment: • Alternatively to the analysis, it can be ensured by appropriate precautions that drop of a fuel assembly into the reactor core is prevented.
S3-12	Drop of a fuel assembly onto the reactor core	R	E	Additional boundary condition: • Demonstration of subcriticality with fuel assembly lying on the core.
S3-13	Inadvertent withdrawal of control elements during loading	R, K, VM	E	Comment: • Alternatively to the demonstration of subcriticality, precautionary measures can be taken ensuring that unplanned withdrawal of control elements during loading of the reactor is prevented and allow loading only if all control elements are inserted.
S3-14	Inadvertent withdrawal of a control element during zero-power test or during shutdown safety test	R, K	C, E	

No.	BWR events	Fundamental safety functions concerned	Operational mode	Additionally comments, boundary conditions and notes
S3-15	Wrong loading of the reactor core with more than one fuel assembly	R, VM	E	Comment: • Alternatively to the demonstration of subcriticality, precautionary measures can be taken ensuring that a wrong loading of the reactor core with more than one fuel assembly is prevented.
S3-16	Nuclear-thermal hydraulic instability	R, K	A	Additional boundary condition: • The boundary conditions of the potential initiating events shall be considered. • No consideration of limitation measures. • In-phase and out-of-phase oscillations shall be analysed. • Effectiveness of reactor protection system measures for the early detection of neutron flux oscillations and reactor shutdown shall be demonstrated.
S3-17	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				
S3-18	Leak/break within the containment (leak cross section ≤ 0.1F of each considered line)	R, K, B, S	A-B	Additional boundary condition: • In addition to main steam and feedwater lines, all other coolant-retaining systems shall be considered. • Details on the leak and break assumptions and on safety demonstrations are included in Appendix 2. • Further specifications see Annex 5, Appendix 1, A1 (2)

No.	BWR events	Fundamental safety functions concerned	Operational mode	Additionally comments, boundary conditions and notes
S3-19	Leak/break within the containment (leak cross section > 0.1F of each considered line)	R, K, B, S	A-B	Additional boundary condition: • In addition to main steam and feedwater lines, all systems carrying coolant shall be considered. • Details on the leak and break assumptions and on safety demonstrations are included in Appendix 2. • The double-ended break of a main steam line (“2A break“) shall be analysed for the design of the pressure suppression system, of the reactor pressure vessel 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 safe- ty-relevant systems and components required for the control of the event. • Further specifications see Annex 5, Appendix 1, A1 (2)
S3-20	“80 cm^2“ leak in reactor pressure vessel bottom	R, K, B, S	A-B	
S3-21	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 shall be postulated. The leak size is determined by the largest free cross section in the lines connected with the reactor coolant system. • The analysis shall consider that at the time of onset of the accident a fuel assembly is being 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).

No.	BWR events	Fundamental safety functions concerned	Operational mode	Additionally comments, boundary conditions and notes
S3-22	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 shall be postulated. Note: • Might be relevant for establishment of the sump function and procedures.
S3-23	Leak in reactor pressure vessel bottom due to • inadvertent pulling of a pump shaft, or • work on control element 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).
S3-24	Leak in exhaust pipe of a safety and relief valve within the gas space of the wetwell.	K, B, S	A-B	
S3-25	Loss of tightness between drywell and wetwell	R, K, B, S, VM	A-B	Comment: • Alternatively to the safety demonstration of the control of the event, pre-cautionary measures can be taken so that impermissi-ble leaks between drywell and wetwell, in particular during restart of the plant and after maintenance measures, are prevented.

No.	BWR events	Fundamental safety functions concerned	Operational mode	Additionally comments, boundary conditions and notes
Loss of coolant outside the containment				
S3-26	Leak/break in the main steam or feedwater system and other high-energy piping systems between containment and the first isolation provision outside the containment	R, K, B, S, VM	A-B	Additional boundary condition: • Details on the leak and break assumptions and on safety demonstrations are included in Appendix 2. Special consideration of: • the integrity of the containment, • humidity, pressure build-up, differential pressures, temperature, jet and reaction forces, etc. with redundancy-wide impacts, and • the integrity of safety-relevant structures of the reactor building. Note: • With regard to the VM option see Annex 3 of the „Safety Requirements for Nuclear Power Plants“, Section 3.2.4.
S3-27	Leak/break in the main steam or feedwater system within the turbine building	R, K, B, S	A-B	Additional boundary condition: • For details on the leak or break assumptions and on the required safety demonstrations, see Appendix 2.
S3-28	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. • Spiking effect shall be considered.
S3-29	Leak/break in the reactor water clean-up system in the reactor building	S	A-E	Additional boundary condition: • Spiking effect shall be considered.
S3-30	Leak/break in coolers, carrying reactor coolant, in case of demand	B, S	A-E	
S3-31	Leak in the wetwell	K	A-B	Additional boundary condition: • Details on the leak and break assumptions and on safety demonstrations are included in Appendix 2. • The event is relevant for the transition to residual heat removal via the residual heat removal train from the reactor pressure vessel and a flooding of reactor building (see Annex 3 Section 3.2.2).

No.	BWR events	Fundamental safety functions concerned	Operational mode	Additionally comments, boundary conditions and notes
S3-32	Leak/break in reactor scram system in the reactor building	R	A	Note: • Relevant for the design of the reactor scram system.
S3-33	Leak in residual heat removal system in the reactor building during residual heat removal operation	K, B, S	C-E	Additional boundary condition: • Details on the leak and break assumptions and on safety demonstrations are included in Appendix 2. • Spiking effect shall be considered.
S3-34	Loss of coolant from the reactor coolant pressure boundary into the reactor building via systems connected	K, B, S	A-C	
Release of radioactive material from nuclear auxiliary systems				
S3-35	Leak/break in a pipe or break of a filter in the off-gas or gas treatment system	S	A-F	
S3-36	Leak in tank with active medium	S	A-F	Note: • The tank with the largest radiological hazard potential shall be identified. • The analysis shall consider containment failures resulting from earthquakes.
Loss of energy supply				
S3-37	Loss of offsite power for more than 10 hours	R, K, B, S	A-E	Additional boundary condition: • The shutdown under loss of offsite power conditions shall also be analysed.
Events due to internal hazards				
S3-38	Potential activity release due to plant internal fires (including filter fire) or explosions	S,VM	A-F	Additional boundary condition: • Analyses on fires and explosions affecting components or system areas with high activity release potential shall be performed. Comment: • Optionally, to demonstrate that fundamental safety function K is fulfilled, it may be shown that relevant radiological effects are excluded due to existing fire protection and blast protection measures.

No.	BWR events	Fundamental safety functions concerned	Operational mode	Additionally comments, boundary conditions and notes
S3-39	Break of a control element nozzle with control element ejection.	R, K, B, S	A-B	Additional boundary condition: • In addition to the control of the resulting leak it shall be demonstrated that the ejection of the control element does not lead to an impermissible damage of the containment. Further, it shall be demonstrated that no consequential damage of neighbouring drives occur that impair the functional safety of other control elements. If consequential damage cannot be excluded, it shall be demonstrated that the acceptance criteria are fulfilled anyhow.
Level of defence 4				
Level of defence 4a				
Anticipated transient without scram (ATWS)				
S4a-01	Loss of main heat sink, e.g. by loss of con- denser vacuum or closure of the main steam bypass valve with available auxiliary power supply.	R, K, B	A	Note: • For the analysis of ATWS it may be assumed that the electromagnetic insertion of the control elements is effective.
S4a-02	Loss of main heat sink with unavailable auxiliary power supply	R, K, B	A	
S4a-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	
S4a-04	Total loss of main feedwater supply	R, K, B	A	
S4a-05	Maximum reactivity insertion by withdrawal of control elements or control element groups starting from full power and from “hot zero power condition”	R, K, B	A	
S4a-06	Maximum decrease of the feedwater temperature	R, K, B	A	
S4a-07	Steam line isolation with available auxiliary power supply	R, K, B	A	

No.	BWR events	Fundamental safety functions concerned	Operational mode	Additionally comments, boundary conditions and notes
S4a-08	Steam line isolation with unavailable auxiliary power supply	R, K, B	A	
S4a-09	Maximum increase of feedwater flow rate	R, K, B	A	
S4a-10	Start-up of the recirculation pumps with maximum speed gradient	R, K, B	A	

Table 5.3: Event list fuel storage PWR and BWR

No.	Fuel assembly handling and storage events for PWRs and BWRs	Fundamental safety functions concerned	Operational mode	Additionally considered boundary conditions and notes
Level of defence 2				
Reduced heat removal from the spent fuel pool				
B2-01	Loss of one train in operation or unplanned short-term (max. 30 min) interruption of heat removal	K	A-F	
Loss of coolant from the spent fuel pool				
B2-02	Leakage from the spent fuel pool or water loss via connecting pipes (max. cross section according to DN25)	K	A-F	
Loss of energy supply				
B2-03	Loss of offsite power equal or less than 10 hours	K	A-F	
Reactivity changes in the spent fuel pool				
B2-04	Disturbances in the boron concentration (only PWR)	R	A-F	Note: • Only relevant in case of boron credit in the storage design.
B2-05	Most unfavourable wrong loading of the spent fuel pool or transport and storage cask with a most reactive fuel assembly	R	A-F	
Level of defence 3				
Reduced heat removal from the spent fuel pool				
B3-01	Loss of two trains of the spent fuel pool cooling system for a longer period (> 30 min.)	K	A-F	Additional boundary condition: • For the safety demonstration, grace times and repair possibilities might be taken into account for all operational modes.

No.	Fuel assembly handling and storage events for PWRs and BWRs	Fundamental safety functions concerned	Operational mode	Additionally considered boundary conditions and notes
Loss of coolant from the spent fuel pool				
B3-02	Loss of coolant from the spent fuel pool due to leaks with a cross section > DN25 up to the largest connecting pipe	K, B	A-F	Additional boundary condition: • Maximum cross-sectional area: area of the largest connecting pipe.
B3-03	Leak at the refuelling cavity or setdown pool with opened refuelling slot gate	K, B, VM	E	Additional boundary condition: • Impacts of leaks which may arise during refuelling shall also be considered. Comment: • For the compliance with the fundamental safety functions K and B, there is the option of demonstrating that, due to precautionary measures safety-relevant water losses with opened refuelling slot gate are excluded. See also D3-29 and S3-22 to S3-29 events.
B3-04	Internal leak in heat exchangers of the spent fuel pool carrying coolant	K, B, S	A-F	
Loss of energy supply				
B3-05	Loss of offsite power for more than 10 hours	K, S	A-F	
Reactivity changes during fuel storage				
B3-06	Water/steam ingress in the dry storage facility for non-irradiated fuel	R	A-F	Specification of the acceptance criteria: • $k_{eff} < 0,98$
B3-07	Geometry changes due to external hazards (spent fuel pool, dry storage facility for non-irradiated fuel)	R, K, B	A-F	Note: • See Annex 3 of the “Safety Requirements for Nuclear Power • Plants“, Section 4.2.1.1.
B3-08	Drop of a fuel assembly into the spent fuel pool	R	A-F	Additional boundary condition: • A dropped-down fuel assembly is lying on the storage racks or standing directly adjacent to a storage rack.

No.	Fuel assembly handling and storage events for PWRs and BWRs	Fundamental safety functions concerned	Operational mode	Additionally considered boundary conditions and notes
B3-09	Wrong loading of the spent fuel pool or the transport and storage cask with more than one fuel assembly	R, VM	A-F	Comment: • Alternatively to the verification of subcriticality, precautionary measures can be taken ensuring that a wrong loading of the spent fuel pool with more than one fuel assembly is prevented.
B3-10	Boron dilution in the spent 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 assemblies				
B3-11	Fuel assembly damage during handling	S	A-F	Additional boundary condition: • Damage of all fuel rods at exterior side of a fuel assembly shall be postulated. Note: • The analysis serves to verify that the release into the environment resulting from the release of radionuclides in the containment with- out loss of coolant is sufficiently limited.

Appendix 1:
Principal assignment of load levels to levels of defence and redundancy-wide impacts

Note:
In the event lists, events are assigned to the levels of defence defined in the “Safety requirements for Nuclear Power Plants”. For the reactor coolant pressure boundary and the external systems, load cases and load case classes (these are dimensioning or design load cases, assembly load cases, normal and abnormal operational load cases, test load cases and accidents) are grouped in the KTA safety standards into load levels (0, A, B, C, D, P) to which the permissible stresses are assigned without having made reference to events or levels of defence so far. Only in the KTA Safety Standard “Steel Containment Vessel”, events to be assigned to load levels 0, 1, 2, 3 are stated. However, these are not assigned to levels of defence. For events of the event lists assigned to the fundamental safety function “Confinement of radioactive materials” the respective load levels are included in the following matrix. The load levels for the components defined in the KTA standards are assigned there to the levels of defence. These load levels shall be applied according to the limitation of consequential impacts on components affected by the postulated events.

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 requirements are 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 both the load cases as well as 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 sets of requirements for the steel containment vessel are stated in KTA Safety Standard 3401.2. There is no KTA standard for the containment of pre-stressed concrete with steel liner, so that no load levels are stated here.

A1 (1) The assignment of load levels to levels of defence or to redundancy-wide impacts shall be performed plant-specifically such that all systems, including the system interfaces 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 shall be 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 level		
	Reactor coolant pressure boundary	**External systems**	**Steel containment vessel**
Design level / Level of defence	0	0	0
1	A/P	A/P	1/2
2	B	B	1/2
3	C[1) 3)]/D[5)]	B[4)]/C[3)]/D[2)]	1/2/2
4a	C[3)]	B[4)]/D[5)]	1
Redundancy-wide impacts and very rare human-induced external hazards			
Design basis earthquake[3)]	D/C[6)]	D/C[6)]	3
Aircraft crash and explosion blast wave[3)]	D/C[6)]	D/C[6)]	3[7)]

1) Except for a large leak at the reactor coolant pressure boundary within the containment.

2) For leaks > 0,1A within the containment: Load level D is not permissible if, subsequently, use of the component is required for the control of the accident.

3) For the case that an impairment of functional performance cannot be excluded, a verification of functional performance shall be provides that also comprises a longer-term safe plant condition after the occurrence of the impact. Alternatively, the loads on Level B may be restricted for the reactor coolant pressure boundary and the external systems.

4) For loads resulting from the operation of the safety system.

5) Functional capability shall be verified for components necessary for the control of the event.

6) Meeting level C might be necessary if the integrity of the components, especially of the pipe connections, cannot be guaranteed when meeting level D. Aftershocks shall be considered in case of impacts by earthquakes.

7) For the load cases “aircraft crash” and “explosion blast wave”, the integrity for the undisturbed areas of the containment shall be demonstrated.

8) Regarding seismic impacts, aftershocks shall also be considered depending on the site-specific conditions.

Appendix 2: Postulated leak cross sections and breaks in the reactor coolant pressure boundary and in the external system

1 Principles and prerequisites

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

Note:
The requirements in Sections 2.1 and 3 are structured according to the following acceptance targets:

- Maintenance of fuel assembly cooling by compensating the loss of coolant (design of the emergency core cooling systems),
- Ensuring a reactor core geometry that can be shutdown and cooled,
- Prevention of damage propagation 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.

1 (2) The application of this Appendix requires the fulfilment of the „Safety Requirements for Nuclear Power Plants“, Section 3.4.

1 (3) For the piping systems not dealt with in the following sections, a 2A break shall be postulated (A = open cross-sectional area).

2 Reactor coolant pressure boundary of PWRs

2.1 Main coolant line including connecting lines DN > 200

Maintenance of fuel assembly cooling by compensating the loss of coolant (design of the emergency core 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 shall be taken as a basis. The emergency core cooling systems shall be designed accordingly.

Ensuring a reactor core geometry that can be shut down and cooled.

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 shall be postulated for different leak positions.

Prevention of damage propagation

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 shall be postulated. This also applies to the determination of releases of material resulting from jet forces with regard to potential impairment of emergency core 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 shall be 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 shall apply:

The support stability of these components shall be ensured for the static equivalent force P_{ax} which shall be superposed with the own weight of the component:

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

with

p = operating pressure at full power

F = 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 shall be demonstrated separately for each nozzle.

Note:
For the steam generator, support stability shall be ensured in the same way as for the connection to the secondary circuit. This is dealt with under the leak postulates of the main steam and feedwater lines.

2.1 (6) Design pressure and design temperature for fault-proof electrical equipment shall be 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 shall be 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 reactor pressure vessel internals and the design of the emergency core cooling system, a leak in the reactor pressure vessel with a size of about 20 cm^2 (geometric cross section: circular) below the upper edge of the reactor core shall also be postulated.

2.2 (2) The design of the reactor pressure vessel internals and of the protection measures for the containment shall also consider the consequences of a sudden break of a control element drive, control element travel housing 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) shall be determined. It shall be demonstrated that the steam generator tubes withstand these loads.

2.3 (2) Regarding the accident analyses for the main steam line break and the inadvertent opening of a main steam safety valve, however the failure of some few steam generator tubes shall be postulated as random failure and not as additional failure resulting from these events which shall be 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 needs not to be postulated in these accident analyses.

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 needs not to be 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 needs not to be postulated.

2.3 (5) If postulating subcritical cracks or the rupture of a small-bore line, no addition- al steam generator tube failure needs to be superposed.

3 Reactor coolant pressure boundary of BWRs

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

3 (1) The analysis of the effectiveness of emergency core cooling and the design of the emergency core cooling systems shall be 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 cm^2 (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 element drive or the weld between housing tube and reactor pressure vessel.

Ensuring a reactor core geometry that can be shutdown and cooled

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 subsection 3 (1) b).

Prevention of damage propagation

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 stationary discharge flow for different leak positions to be considered shall be postulated. This also applies to the determination of releases of material resulting from jet forces with regard to potential impairment of emergency core cooling by these materials, postulating the most unfavourable leak positions and sizes (≤ 0.1 A).

3 (4) For the prevention of pressure built-up in the gas space of the wetwell due to a leakage in the exhaust pipe with a 0.1 A cross section to be postulated between wetwell ceiling and the discharge area of the exhaust pipe inside the water pool provisions shall be made - as far as required - e.g. an guard pipe around the exhaust 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 shall be considered in the design basis. Here, a guillotine break (2A break) with linear opening behaviour and an opening time of 15 ms shall be postulated as input parameter for the calculation. With this assumption, analyses of dynamic loads resulting from subcritical cracks do not need to be performed.

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

The support stability of these components shall be ensured for the static equivalent force P_{ax} which shall be superposed with the own weight of the component:

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

with

p = operating pressure at full power

F = 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 of the reactor pressure vessel shall be dimensioned such that also the leaks postulated according to subsection 3 (1) b) are covered.

3 (8) For the determination of design pressure and design temperature for fault-proof electrical equipment, 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 shall be 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 shall be postulated. These shall be calculated on the basis of fracture mechanics or limited to 0.1 A.

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 shall be 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 shall be considered in the design basis. Here, a guillotine break (2A break) with linear opening behaviour and an opening time of 15 ms shall be 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 shall 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

F = 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.

4.2 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 shall apply as far as these pipes are located in the reactor building:

- Subcritical cracks in the welds. The resulting leak cross sections shall be 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 shall be considered if one of the criteria a1) or a2) applies:

  a) 1. operating pressure[1)] ≥ 20 bar or
     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.

1) Load Level A has to be considered, see Appendix 1.

4.2 (2) If a guillotine break shall be postulated in accordance with the criteria mentioned, the proceeding with regard to the consequential effects is as follows:

- For the determination of differential pressures and jet forces on building parts, unimpeded discharge flow shall be postulated.
- For the calculation of an internal blast wave for determination of the loads of internals, unimpeded discharge flow shall be 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 shall be postulated.

4.2 (4) For pipes with a diameter smaller than DN 50 and all pipes outside the reactor building, double-ended breaks shall be postulated in general.

5 Vessels, valve and pump casings

For those vessels (other than reactor pressure vessel), heat exchanger and valve and pump casings (including the pertinent casings 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 Requirements for Nuclear Power Plants“, Section 3.4) were presented, the respective leak and break postulates of the connecting pipes at their connecting point shall be assumed. For vessels, heat exchangers and other components witch several connections, the most unfavourable leak shall be considered in dependence of the acceptance target, taking into account the leak and break postulates for the selected connecting pipe.

Bursting of vessels (other than the reactor pressure vessel), heat exchangers and valve and pump casings shall generally be postulated.

Annex 3 of the

"Safety Requirements for Nuclear Power Plants":

Requirements for the protection against internal and external hazards as well as very rare human-induced external hazards

22 November 2012

Structure

1 Fundamental requirements on protection concepts for internal and external hazards as well as very rare human-induced external hazards

1 (1) All equipment required for safe shutdown of the nuclear reactor, for maintaining it in a shutdown state, for residual heat removal or for prevention of the release of radioactive materials shall be designed and constantly kept in such a condition that they can fulfil their safety related tasks even in case of any internal and external hazard including very rare human-induced external hazards.

Note:
Requirements for this equipment to be considered with regard to malevolent disruptive acts or other third party intervention are not covered by the “Safety Requirements for Nuclear Power plants”.

1 (2) The safety system as well as the emergency equipment shall be designed such that they remain effective in the event of internal and external hazards. The fundamental design requirements for safety equipment with respect to these hazards are contained in the corresponding regulations in Section 2.4 of the "Safety Requirements for Nuclear Power Plants".

Precautionary measures

1 (3) Precautionary measures shall ensure that internal or external hazards including very rare human-induced ones impairing the required function of safety equipment shall be

- either prevented
- or sufficiently limited in their effects (see also "Safety Requirements for Nuclear Power Plants" subsection 2.1 (5)).

1 (4) The requirements for effectiveness and reliability of precautionary measures depend on the estimated occurrence frequency of those hazards, against which the protection is provided, and on the potential effects of these hazards.

1 (5) If precautionary measures as described in Sections 3, 4.2.1 and 4.2.3 are in place, analyses of event sequences due to the corresponding internal and external hazards are not required. Hence, the safety demonstration focuses on compliance with the requirements for effectiveness and reliability of the precautionary measures.

For events on level of defence 3 that are nevertheless postulated to occur due to such hazards, the requirements of this level of defence shall apply.

1 (6) Radiological consequences shall be determined for those events originating from hazards according to subsection 1 (5) leading to a radiologically representative event on level of defence 3.

Note:
Radiologically representative events on level of defence 3 are listed in Annex 2 of the "Safety Requirements for Nuclear Power Plants". Specific provisions regarding the determination of radiological consequences are referred to in the event-specific requirements in Sections 3 and 4 further below.

Very rare human-induced external hazards

1 (7) Very rare human-induced external hazards according to Section 4.2.2 shall not inadmissibly impair the required function of safety equipment. Otherwise specifically designed features shall be in place to prevent event sequences on level of defence 4b.

When analysing very rare human-induced external hazards and the postulated consequential events, realistic initial and boundary conditions as well as realistic

models may be applied (see also "Safety Requirements for Nuclear Power Plants", Annex 5, Section 3.2.1).

1 (8) Requirements with regard to redundancy of equipment for the control of very rare human-induced hazards and the postulated consequential events are provided in the "Safety Requirements for Nuclear Power Plants", Annex 4, Section 2.4.

1 (9) In case the main control room is inoperable as a result of a very rare human-induced external hazard, it shall be ensured that the plant is brought into a controlled plant state without any manual intervention and can remain in this state for at least 10 hours by means of emergency equipment. Moreover, the plant shall be brought into a state which ensures subsequent residual heat removal in the long-term via a residual heat removal system. Measures need not be automated if a sufficient grace period is available or administrative measures are in place for their actuation. For long-term control of very rare human-induced hazards, on-site supporting measures can be taken.

1 (10) The following requirements apply to emergency equipment:

a) Components and sub-systems of the emergency equipment shall be protected against the postulated very rare human induced external hazards.

b) It shall be ensured that the required functions of the emergency equipment cannot be impermissibly impaired by damage in plant areas which are not protected against the hazard under consideration. This does include also energy supply systems and I&C equipment.

c) It shall be ensured that unauthorised interventions or operating errors in the main control room or in other plant areas which are not specifically protected do not lead to any inadmissible impact on the required function of the emergency equipment.

d) Interventions, which might lead to any inadmissible impact on the required function of the emergency equipment are neither permitted for operational reasons nor for inspection purposes, if they cannot be withdrawn or completed in case of a very rare human-induced hazard. This does not apply if equivalent functions are in place.

1 (11) In the event of very rare human-induced external hazards resulting from "aircraft crash" and "explosion pressure wave" cooling of the fuel assemblies shall be ensured in the long-term. Repair measures at equipment required in the long-term, shall be performed in due time, if required.

Accessibility of those areas where local actions may be carried out shall be ensured as well as the communication with the personnel working in these areas.

2 Requirements for precautionary measures

2 (1) Reliability and effectiveness of precautionary measures shall be such that the requirements according to subsections 1 (2), 1 (3) and 1 (4) are met.

2 (2) Precautionary measures shall be mainly based on passive means. If inadmissible consequences cannot be reliably prevented by passive means, reliable active means shall be in place. If administrative measures are taken, their reliability has to be demonstrated according to subsection 2 (6). If in an exceptional case precautionary measures are exclusively based on administrative measures, their reliability shall be thoroughly justified.

2 (3) The effectiveness of precautionary measures shall be ensured even if the single failure concept is applied (see Annex 4 of the "Safety Requirements for Nuclear Power Plants").

2 (4) During maintenance including in-service inspections, reliability and effectiveness of precautionary measures shall not be inadmissibly impaired.

2 (5) Postulated malfunction of or damage to precautionary measures as well as their faulty operation or human error in the execution of precautionary measures according to Annex 2 and Sections 3 and 4 below shall not impair the function of the safety system, of the emergency equipment as well as of further equipment necessary for safety.

2 (6) If administrative measures and related operator actions are part of precautionary measures, their effectiveness and reliability shall be demonstrated by methods such as failure mode and effect analysis or hazard analysis. In particular, systematic failures shall be considered.

The following conditions shall be ensured:

- Distinct organisational provisions shall be specified regarding competence and responsibility for execution and checking of precautionary measures. The personnel responsible for performing and checking precautionary measures shall be specially qualified in accordance with the safety significance of the precautionary measures.
- Distinct procedures and instructions for execution and check of precautionary measures shall be in place. Type and number of the checks shall be specified in accordance with requirements regarding reliability of the respective precautionary measure. Distinct, measurable and quantifiable criteria shall be specified for the checks. Any safety implications of identified deviations from these requirements shall be assessed.
- The execution of checks and the results obtained shall be comprehensively documented. The persons involved shall be indicated.
- Sufficient time shall be available for performing and checking precautionary measures.
- Environmental conditions shall not impair conducting and checking precautionary measures.
- The boundary conditions under which the persons in charge carry out/conduct precautionary measures shall ensure the prerequisites for failure-free behaviour to the extent possible. Ergonomic requirements according to subsection 3.1 (13) of the "Safety Requirements for Nuclear Power Plants" shall be considered.
- Potential errors and their consequences shall be considered in the training of the personnel.

2 (7) Validity of the boundary conditions for the effectiveness and reliability of precautionary measures shall be ensured over the entire plant operating lifetime.

3 Requirements for internal hazards

3.1 General requirements

3.1 (1) Plant specifically identified and evaluated internal hazards as well as their potential combinations or their combinations with external hazards including very rare human-induced ones shall be fully considered.

Note:
See also Sections 2.4 and 4.2 of the "Safety Requirements for Nuclear Power Plants" and subsections 3.2.1 (3) and (4) of Annex 5 of the "Safety Requirements for Nuclear Power Plants".

3.1 (2) For each hazard or combination of hazards according to subsection 3.1 (1), the safety related impacts on the plant under consideration shall be determined considering the consequential impacts to be expected. In particular, the effects listed in the following shall be considered:

- Plant internal flooding,
- Plant internal fires and explosions,
- Increased radiation levels,
- Chemical reactions,
- Electrical, I&C or process-related malfunctions/failures,
- Pressure build-up, pressure differences,
- Temperature and humidity increase,
- Fragments (debris/missiles) flying around and falling, as well as
- Jet and reaction forces.

3.1 (3) Features for the protection against internal hazards shall preferably be installed close to the potential source of an internal hazard unless any other location is more advantageous with regard to safety.

3.2 Hazard specific requirements

3.2.1 Plant internal fire

3.2.1 (1) Protection features and measures for the protection against plant internal fires and their consequences shall be in place both inside and outside of buildings. Inadmissible impacts of fires and their consequences shall be prevented by active and passive fire protection means.

3.2.1 (2) Fire protection measures and equipment (means) shall be planned and implemented such that defence in depth is realised:

- Suitable protection means shall be in place to prevent the occurrence of incipient fires.
- Fires which have nevertheless occurred shall be quickly detected and suppressed.
- The propagation of any fire neither extinguished nor self-extinguished shall be limited.

3.2.1 (3) A fire protection concept shall be developed and documented. The documentation shall be kept up to date. In case of any plant modification, its effects on the existing fire protection concept shall be assessed and enhanced, if necessary.

3.2.1 (4) A fire hazard analysis shall be performed and documented. The documentation shall be kept up to date.

3.2.1 (5) The entire fire protection means shall ensure that even in case of a random failure of a single fire protection means the required safety functions are not inadmissibly impaired.

3.2.1 (6) An ignition of combustibles shall be postulated in principle. Deviations from this requirement are admitted, if the combustible is encapsulated and it has been demonstrated that the encapsulation maintains its operability during specified normal operation as well as in case of any postulated accident (including those resulting from fire).

3.2.1 (7) Fire loads and potential ignition sources shall be limited to the degree necessary for safe operation.

3.2.1 (8) For prevention of an ignition by potential ignition sources, fire loads needed for plant operation shall be sufficiently physically separated from the ignition sources referred to in subsection 3.2.1 (7) at any location, where permitted by design or requirements for the operation of items important to safety.

Plant areas containing considerable fire loads shall be principally separated by sufficiently rated fire barriers.

3.2.1 (9) Redundant trains of the safety system shall be in principle separated by sufficiently rated fire barriers to prevent a loss of more than one redundant train in case of fire.

If the protection required in the event of fire cannot be ensured by structural protection means due to systems engineering or operational reasons, an equivalent level of protection shall be ensured by other (compensatory) fire protection means or by a combination of different fire protection means.

3.2.1 (10) For transient combustibles in connection with maintenance work special protection means shall ensure that the plant safety is not inadmissibly impaired.

3.2.1 (11) Passive structural fire protections means shall ensure the fire safety of buildings and structures.

3.2.1 (12) In principle, only non-combustible constructions and structural elements shall be used. The use of combustible materials is only permissible if the use of such materials cannot be avoided, e.g. insulation materials for cooling pipes, decontaminable coatings. In principle, only non-combustible operating supplies shall be used. Exceptions are control and lubricating fluids as well as other combustibles materials that cannot be avoided for operational reasons.

3.2.1 (13) In principle, I&C wires and cables should be routed separately from heated pipes or pipes carrying combustible media. Power cables shall be sufficiently separated from signal and control cables.

In case of unavoidable crossings of I&C wires and cables with high- temperature pipes or pipes carrying combustible media or with power cables, particular protection shall be in place.

Adequate protection shall ensure that even in case of fire cables for power supply or I&C cables are not inadmissibly impaired.

3.2.1 (14) The restrictions for the controlled area shall be considered in the selection and installation of active and passive fire protection means.

3.2.1 (15) In the event of fire, particularly in plant areas with equipment of the safety system and in controlled areas, adequate protection shall ensure a reliable and fast fire detection and alarm.

3.2.1 (16) Adequate protection means for fire detection, alarm and suppression shall ensure that fires in the containment can be rapidly and reliably detected and extinguished efficiently, even without smoke removal.

3.2.1 (17) Adequate protection means for a timely detection and alarm of any hazard and appropriate precautions for rapid escape and rescue activities via escape and rescue routes shall ensure that in case of danger persons can reach the outside quickly and can be rescued from the outside.

3.2.1 (18) Escape and rescue routes shall be in place within the buildings. These shall be protected against fire effects for an appropriate time period to allow for self-rescue, rescue of persons, fire extinguishing as well as for personnel actions required for safety reasons.

3.2.1 (19) In principle, stationary fire extinguishing systems shall be actuated automatically. Remote controlled or local manually actuated extinguishing systems are permissible, if the fire effects are controlled until these extinguishing systems come into effect.

3.2.1 (20) Automatically actuated stationary extinguishing systems shall be designed and secured in such a way that neither disturbances occurring at them or at parts of them nor faulty actions/maloperations do neither impair the required function of equipment of the safety system nor the separation of fire compartments.

3.2.1 (21) The entire fire protection means shall regularly be subject to in-service inspections with respect to their required function. Test intervals shall be specified according to the safety significance of the equipment to be protected.

3.2.1 (22) For fire suppression, an efficient professional on-site fire brigade shall be established, equipped and maintained according to the existing non-nuclear regulations. In addition, the local off-site fire brigade shall be familiarised with the plant and the different plant areas as well as with the specific boundary conditions at a nuclear power plant. The corresponding instructions shall be repeated at regular intervals. Fire drills shall be conducted at appropriate time intervals.

3.2.1 (23) It shall be ensured that all means required for ensuring safe operation and control of events on levels of defence 3 and 4a can also be taken in case of fire suppression.

3.2.2 Plant internal flooding

3.2.2 (1) Adequate protection means shall be in place for the prevention of plant internal flooding. These include:

- High-quality design of the medium-containing systems and components,
- Precise specifications for maintenance measures on medium-containing systems and components, in particular those with high flooding potential,
- High reliability of stationary automatic fire extinguishing systems with respect to inadvertent actuations.

3.2.2 (2) Potential initiating hazards for plant internal flooding shall be identified in the frame of a flooding analysis (e.g. leaks, actuation of a fire extinguishing system, human errors, drop or strike of loads, start-up of systems after maintenance measures or plant modifications with isolation devices inadvertently not installed). It is possible to define an enveloping hazard as design basis for precautionary measures.

3.2.2 (3) Water accumulations at structures located on an elevated level (e.g. cable racks with insufficient drainage) shall be considered in the frame of the flooding analyses.

3.2.2 (4) The possibility of clogging of drainage structures and of displacement of objects and wash up of small particles shall be considered.

3.2.2 (5) For determination of the flooding level and of the mechanical impacts on components or barriers, potential formation of waves shall be considered.

3.2.2 (6) For all postulated flooding hazards, the anticipated time history of the water level in the rooms affected directly as well as in potentially affected adjacent rooms shall be considered.

3.2.2 (7) In addition to the direct impact of flooding, indirect effects, such as increased humidity, shall also be considered.

3.2.2 (8) A possible pressure increase due to the contact of water with hot components shall be considered.

3.2.2 (9) For all postulated flooding hazards, protection means for prevention of inadmissible effects on the safety system shall be in place. In this context, the following protection means shall be considered, in particular, according to a graded approach:

- Leak monitoring systems,
- Means for the detection and isolation of leak locations,
- Installation of items important to safety on an elevated level,
- Structural provisions (e.g. drainage pans, barriers) enclosing or separating items important to safety,
- Guard pipe design,
- Bars or equivalent structures for preventing spread of water, in particular into adjacent redundant trains,
- Active or passive drainage features,
- Organisational means in the event of flooding.

3.2.2 (10) During maintenance on prevention means against flooding, their required function shall either be ensured or fully compensated by other means. In particular, the sump suction lines and their isolation valves, lines with a high fill-up potential and their isolation devices, equipment for prevention of flooding of more than one redundant train in the reactor annulus of PWR plants as well as maintenance work in the bottom area of reactor pressure vessels of BWR plants in connection with maintenance activities shall be considered.

3.2.3 Component failure with potential impacts on items important to safety

3.2.3 (1) As far as a component failure and consequential endangerment of equipment of the safety system cannot be prevented, precautions shall be in place for the protection of this equipment.

3.2.3 (2) All potentially safety significant sources of (high energetic) fragments (debris) flying around and falling shall be identified. The parameters (in particular geometry, mass and trajectory) of the fragments to be expected in case of failure shall be analysed or assessed conservatively.

The following potential sources of such fragments shall particularly be considered:

- Failure of vessels, pipes and other components with high energy content,

Note:
For the leak and break postulates, see Appendix 2 in Annex 2 of the "Safety Requirements for Nuclear Power Plants".

- Failure of mobile valve components,
- Ejection of a control element or control rod, and
- Failure of rotating component parts (e.g. flywheel failure of the reactor coolant pumps, turbine blades, turbine shaft).

3.2.3 (3) The required function of equipment of the safety system shall be ensured according to subsection 1 (2) in case of impacts resulting from a postulated component failure, e.g.:

- Direct mechanical impacts (reaction forces, pipe whip),
- High energy fragments,
- Jet forces,
- Plant internal flooding,
- Increased humidity,
- Physical or chemical impacts,
- Pressure differences (static and dynamic),
- Increased room temperature, and
- Increased radiation level.

3.2.3 (4) As far as necessary, mechanical stability of plant components shall be ensured in case of impacts from these hazards.

3.2.3 (5) The following protection means against impacts resulting from a component failure shall be considered:

- Appropriate orientation of the components in the compartment identified as potential source of fragments,
- Appropriate spatial layout of the equipment of the safety system identified as potential targets of fragments,
- Selection of building arrangement such that equipment of the safety system is not located within the probable flight direction of potential fragments of the turbine generator set. 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.

3.2.3 (6) Damages of the safety system, of emergency equipment and other equipment of items important to safety due to pipe whip shall be preferably prevented by structural protection means for the pipes.

3.2.3 (7) In the event of a postulated impact in case of a failure of rotating components, reliable means for limiting the speed and vibration monitoring for identification of damages (initiated by unbalances) shall be in place.

3.2.3 (8) Adequate protection means shall ensure that the flywheels of the reactor coolant pumps (PWR) are not destroyed during a loss of coolant accident (LOCA) as a result of rotation speed exceeding limits.

3.2.3 (9) Structural elements for protection against high energy fragments shall consider both the local (e.g. penetration, spalling) and the global load- bearing and deformation behaviour of the structural elements during impact of the fragment.

3.2.3 (10) In the event of a postulated double-ended rupture of a high energy pipe measures against impacts by jet and reaction forces according to Appendix 2 in Annex 2 of the "Safety Requirements for Nuclear Power Plants" on items important to safety according to subsection 3.2.3 (6) shall be taken considering the following aspects:

- Pipe whip direction,
- Items important to safety affected,
- Kinetic energy,
- Amount of energy absorbed by a component affected,
- Effectiveness of pipe whip restraints, and
- Potential consequential effects in case of an impact on other components.

3.2.4 Leak/break in the main steam/feedwater system as well as in other high energy pipes in the annulus and in the valve compartment (PWR) or between containment and first isolation possibility outside containment (BWR)

3.2.4 (1) The impacts of leaks

- in the annulus and in the valve compartment (PWR) in piping systems carrying main steam or feedwater,
- 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

shall neither impair the containment, including the penetrations, as well as equipment of safety system, emergency equipment and further equipment necessary for safety in the area between containment and the reactor building (annulus) and the valve compartment (PWR) nor lead to an inadmissible release of radioactive materials.

3.2.4 (2) Inadmissible impacts shall be prevented by appropriate design of the pipes in this area, e.g. by guard pipe designs.

Note:
See also events D3-06 as well as S3-26 in Annex 2 of the "Safety Requirements for Nuclear Power Plants".

3.2.5 Drop and impact of heavy loads with potential risk for items important to safety

3.2.5 (1) Loads that may lead to the failure of items important to safety or the release of radioactive material when dropped shall be identified. These also include roll-over and impact of swinging objects, in particular of transport and storage casks.

3.2.5 (2) Faulty operation or maintenance on lifting equipment as well as on its hoisting gears, load-bearing and load attachment devices shall also be considered as potential causes of a drop of heavy loads.

3.2.5 (3) A drop of load with inadmissible consequences shall be prevented.

3.2.6 Electromagnetic hazards

3.2.6.1 Protection against electromagnetic interference

3.2.6.1 (1) Equipment of safety system, emergency equipment as well as further equipment necessary for safety shall be reliably effective in their electromagnetic environment.

3.2.6.1 (2) The electromagnetic compatibility (EMC) of equipment according to subsection 3.2.6.1 (1) shall be demonstrated by an analysis (EMC analysis). It comprises i.e. EMC emissions, EMC immunity of components, EMC immunity against self-emitted electromagnetic interferences, and the corresponding necessary tests.

3.2.6.1 (3) During the plant operating lifetime, both the presence of new sources and changes in existing sources of interference shall be monitored and analysed. The protection of equipment according to subsection 3.2.6.1 (1) against electromagnetic interferences shall be adapted to changes in the environmental conditions as far as necessary.

3.2.6.2 Limitation of electromagnetic interference radiation

3.2.6.2 (1) Potential sources of the electromagnetic interferences inside the plant, whose effects on equipment according to subsection 3.2.6.1 (1) cannot be avoided, shall be identified and possible effects from these sources shall be assessed. Enveloping sources of interference shall be analysed to the extent possible. The environmental conditions resulting from operation of the electromagnetic interference sources at the location of these items shall be determined.

3.2.6.2 (2) Electromagnetic interference shall be limited such that required function of the equipment according to subsection 3.2.6.1 (1) is ensured.

3.2.6.2 (3) For limitation of electromagnetic influences from plant internal sources, administrative and technical means shall be in place for protection of I&C equipment according to their safety significance (e.g. shielding, decoupling, grounding, spatial separation).

3.2.6.2 (4) Transient potential sources of electromagnetic interference, e.g. measuring and testing devices, welding equipment or mobile phones, shall be considered.

3.2.6.2 (5) Interference-induced electromagnetic interactions (short circuit, electric arc) shall be considered.

3.2.6.3 Qualification of the equipment regarding their protection against inadmissible electromagnetic interference

3.2.6.3 (1) Equipment according to subsection 3.2.6.1 (1) shall be qualified in their operational environment with regard to the protection against inadmissible electromagnetic impacts (EMC certification).

3.2.7 Collision of vehicles at the plant site with structures, systems or components important to safety

3.2.7 (1) Structures, systems, and components important to safety shall be designed or protected by structures such that their required safety function is not inadmissibly impaired by collisions with vehicles at the plant site.

3.2.8 Multi-unit plant interactions

3.2.8 (1) Internal hazards shall not lead to an inadmissible impact on the safety of the neighbouring unit.

3.2.9 Plant internal explosions

3.2.9.1 General requirements

3.2.9.1 (1) The required functions of the safety system shall be ensured by suitable protection means for explosion protection.

3.2.9.1 (2) Appropriate protection means inside and outside of buildings shall be in place for prevention of chemical and physical explosions inside and outside of buildings on site, as far as the initiating materials are stored or handled in relevant amounts or if they can be produced on site.

3.2.9.1 (3) Explosion protection means shall be planned and designed such that defence-in-depth is implemented. The protection means shall:

- prevent the formation of an explosive gas mixture,
- prevent the ignition of an explosive gas mixture that has been formed despite the provisions, and
- limit the consequences of an explosion such that inadmissible impacts to safety do not occur.

3.2.9.1 (4) If the formation of explosive gas mixtures cannot be prevented, appropriate protection means shall be in place to ensure that the equipment of the safety system is not inadmissibly impaired. These include:

- Minimising the amounts of explosive gas mixtures,
- Eliminating all potential ignition sources, encapsulation of ignition sources, where necessary (exception: installations for decomposition of explosive gas mixtures),
- Adequate ventilation, and
- Use of equipment and tools, in particular electrical devices, qualified for the use in explosive atmospheres.

3.2.9.1 (5) The consequences of postulated explosions shall be minimised by protection means, such as:

- Pressure relief systems,
- Safe distances to equipment of the safety system, and
- Protective features such as (sealing) walls.

3.2.9.1 (6) All postulated explosions shall be assessed regarding their impacts on equipment of the safety system.

3.2.9.1 (7) If explosive materials are necessarily being available at the plant site, the following principles shall be applied:

- The amount of explosive materials shall be minimised.
- Proper storage shall be ensured.
- Sufficient distance to potential ignition sources shall be kept.

– Fire and gas alarm systems and, where appropriate, automatically actuated stationary extinguishing systems shall be in place at the storage location.

3.2.9.1 (8) Pressure waves not resulting from a chemical explosion shall be considered.

Note:
This includes e.g. pressure waves resulting from electric arcs in medium and high voltage electric switchgears.

3.2.9.2 Prevention of inadmissible effects of radiolysis gas reactions in systems and components

Note:
The following requirements are mainly applicable to plants with boiling water reactors.

3.2.9.2 (1) Appropriate means for the prevention of radiolysis gas accumulation and, if necessary, for minimising the consequences or radiolysis gas reactions shall be in place.

3.2.9.2 (2) The protection means to be in place according to subsection 3.2.9.2 (1) shall consider all the system areas that may be impacted by reactor coolant steam.

3.2.9.2 (3) For specifying the system areas affected, all plant operational states, operating processes and conditions of the disturbed operation shall be considered. In particular, the accumulation of radiolysis gas by condensation of steam containing radiolysis gas on cold media shall be considered.

3.2.9.2 (4) If radiolysis gas accumulations cannot be prevented for process-related reasons, radiolysis gas accumulations and reactions shall be postulated for the specification of the precautionary measures to be taken.

The reaction pressure and the impacts on the equipment of the safety system by fragments and blast waves as well as those by loss of coolant, jet forces, increased radiation level, reaction forces, temperature and humidity shall be determined.

3.2.9.2 (5) The effectiveness of the protection means in place shall be continuously monitored and demonstrated by regular in-service inspections.

3.2.9.2 (6) Passive means for ensuring the directed flow shall be preferred to forced flow.

3.2.9.3 Prevention of explosive hydrogen mixtures inside the containment

3.2.9.3.1 General requirements

3.2.9.3.1 (1) 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 3, there shall be a safety margin to the ignition limit of hydrogen (4 % hydrogen in the air) at any time, both integrally and locally. All sources of hydrogen formation shall be considered.

Note:
The specifications to be considered for determining the formation and release of hydrogen in loss-of-coolant accidents are contained in Appendix 1 of Annex 5 of the "Safety Requirements for Nuclear Power Plants".

3.2.9.3.2 Monitoring of the hydrogen concentration in containment compartments after loss-of-coolant accidents

3.2.9.3.2 (1) A measuring system shall be in place to ensure reliably the determination of the hydrogen distribution within the primarily impacted containment areas even under conditions to be expected after a loss-of-coolant accident.

3.2.9.3.2 (2) Based on appropriate calculation methods measuring points shall be defined that enable reliable monitoring of hydrogen concentrations.

3.2.9.3.2 (3) At the measuring points for determining hydrogen concentrations, temperature inside the containment shall also be measured.

3.2.9.3.3 Prevention of explosive hydrogen concentrations after loss-of-coolant accidents

3.2.9.3.3 (1) The following principles shall apply to protection means for prevention of explosive hydrogen concentrations in the containment atmosphere after a loss-of-coolant accident:

- If the calculations reveal that the hydrogen concentration may reach values above the ignition limit in certain containment areas, means to ensure sufficient forced flow mixing of the containment atmosphere shall be in place.
- If the calculation of the integral hydrogen concentration reveals that without any hydrogen depletion measures it cannot be prevented that the ignition limit will be reached in the long-term, the following shall apply:

  (i) The recombiner depletion rate shall be such that the integral hydrogen concentration in case of maximum initial loading by hydrogen, in particular originating from Zr-H_2O reaction, will always remain below the ignition limit.

  (ii) The design of the recombiners shall reliably ensure their availability and operability even under conditions prevailing within the containment at the time of necessary activation. It shall be demonstrated that the fission product load of the recombiners determined under conservative boundary conditions will not inadmissibly impair their required function under radiological aspects and aspects important to safety by airborne halogens and volatile solids and the resulting temperature change in the recombiners.
  (iii) 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 shall be installed as near as possible to the containment with respect to accessibility. This location and other plant areas outside the containment, which are penetrated by the inlet and outlet pipes of the recombiner system, shall be ventilated through aerosol and iodine filters in order to prevent any inadmissible radioactive release through potential leaks. The pipes shall be shielded accordingly.

3.2.9.3.3 (2) It shall be possible to take active measures in due time before a postulated hydrogen concentration of 4 % volume content has been reached. Manual actuation is permitted.

3.2.9.3.3 (3) Credit shall not be given to flushing of the containment (injection into and discharge from the containment) as a measure for reducing the integral hydrogen concentration in the frame of the safety demonstration for accident control.

4 Requirements for external hazards including very rare human-induced external hazards

4.1 General requirements

4.1 (1) Natural as well as human-induced external hazards which have to be considered at the site shall be identified and checked regularly for any possible change.

Note:
See also Sections 2.4 and 4.2 of the "Safety Requirements for Nuclear Power Plants" as well as subsections 3.2.1 (3) und (4) of Annex 5 of the "Safety Requirements for Nuclear Power Plants".

4.1 (2) All hazards identified according to subsection 4.1 (1) shall be included in the analysis. If one hazard also covers other ones, this shall be clearly indicated. Following any modification in the protection means for an enveloping hazard, its covering character shall be re-evaluated.

4.1 (3) A protection concept shall be established to provide a basis for the design of suitable permanent protection means. As part of the protection concept, for each hazard the effects on the plant shall be determined and considered including the development of the hazard over time and all expected consequential effects (such as e.g. the simultaneous occurrence of a pressure wave due to the bursting of vessels with high energy content in the turbine building during an earthquake).

4.1 (4) The protection concept for external hazards including very rare human-induced external hazards shall be documented in a verifiable manner. The documentation shall be kept up to date. It shall contain at least a list of those hazards to be considered as well as a demonstration of the suitability and sufficient reliability of the protection measures taken or equipment provided.

4.1 (5) In general, a permanent effective protection shall be implemented by the protection means in place. With respect to external hazards with a sufficiently moderate development over time, credit can be taken from additional temporary means.

4.1 (6) External hazards including very rare human-induced external hazards and their resulting loads shall in principle be combined with the specified static and dynamic operational loads on the corresponding plant components. Deviations are admissible with respect to short-term and not frequently recurring loads or plant conditions unless a simultaneous occurrence has to be assumed due to their probability and the extent of damage.

4.1 (7) The stability of transport and storage casks shall in principle be ensured for all set-down positions on-site, even in the event of an external hazard or a very rare human-induced external hazard. Exceptions are restricted to unavoidable short-term set-down of the casks during transport and handling processes. The set-down duration on these positions shall be limited to the time needed.

4.1 (8) External hazards including very rare human-induced external hazards shall not inadmissibly impair access to the plant and the possibility to carry out measures important to safety, e.g. accident management measures or fire brigade missions, to such an extent that these can no longer be carried out effectively.

4.1 (9) Continuously or suddenly changing parameters of external hazards as well as derived predictions on the further development of the parameters important to safety shall be monitored and anticipated (e.g. water level and water temperature in the receiving water).

4.1 (10) Where applicable, limits and preceding specified levels (intervention levels) shall be defined to ensure that measures are taken in due time, if these are exceeded.

4.1 (11) Following a hazard that has caused the exceedance of an intervention level, it has to be checked if any inadmissible effects on items important to safety have occurred.

4.1 (12) During long-lasting hazards, safety related inspections shall be performed at appropriate intervals.

4.2 Event specific requirements

4.2.1 Natural hazards

4.2.1.1 Earthquake

4.2.1.1 (1) A design basis earthquake and the associated impacts shall be determined for the site under investigation based on site-specific deterministic and probabilistic seismic hazard analyses. For the determination of the seismic engineering parameters of the design basis earthquake, the intensity and, corresponding to the associated seismo-tectonic conditions, the range of magnitudes, distances and focal depths of the controlling earthquakes shall be indicated. Irrespective of any site specific hazard analysis, the design shall at least be based on the intensity VI EMS/MSK.

4.2.1.1 (2) Regarding the design requirements for equipment of the safety system with respect to a design basis earthquake, the corresponding regulations in Section 2.4 of the "Safety Requirements for Nuclear Power Plants" shall apply.

4.2.1.1 (3) Apart from the vibratory excitation of plant structures, systems and components, changes in the subsoil (like e.g. soil liquefaction or subsidence of the ground) shall be considered.

4.2.1.1 (4) The plant design shall ensure that the failure of equipment not designed against earthquake does not pose any inadmissible effect on equipment of the safety system needed for controlling the design basis earthquake and its effects, i.e. that the equipment of the safety system remains reliably effective as required.

Note:
For the consequential effects to be considered in the event of a design basis earthquake, see Annex 2 of the "Safety Requirements for Nuclear Power Plants", particularly events D3-39, S3-36, B3-07.

4.2.1.1 (5) For the reactor coolant pressure boundary and for the outer systems that are needed to fulfil fundamental safety functions, the behaviour during the design basis earthquake shall be assessed by means of a structure- dynamic analysis. The fulfilment of the fundamental safety functions shall be demonstrated. A simultaneous occurrence of a design basis earthquake and a leak in the pressure boundary shall not be postulated due to design and implementation of the pressure boundary. A simultaneous occurrence of a leak in outer systems shall not be postulated if these are designed to withstand earthquake loads.

4.2.1.1 (6) When demonstrating that long-term sub-criticality is ensured after a design basis earthquake, the effectiveness of the reactor scram system may also be considered for PWR apart from the boron injection equipment with seismic design. In the safety demonstration, the single-failure concept shall be applied.

4.2.1.1 (7) Regarding the design basis earthquake, it shall be demonstrated that the radiological safety objectives associated with level of defence 3 are met.

4.2.1.1 (8) Seismic instrumentation shall be installed by means of which the engineering seismological parameters of relevant earthquakes can be determined. The seismic instrumentation shall be capable of recording several consecutive earthquakes (foreshocks, mainshock, and aftershocks) and reliably indicate any exceedance of limit values for the inspection level of the plant. The records of the seismic instrumentation shall allow statements on all equipment of the safety system. The seismic instrumentation shall allow for a comparison between the design spectrum and the response spectra of registered earthquakes.

4.2.1.1 (9) In the operating procedures, limits of seismic loading shall be defined; if these limits are exceeded, plant inspections and, if necessary, measures (e.g. plant shutdown, assessment of the plant condition) shall be initiated. It shall be ensured that the operating personnel has access to the relevant data from the seismic instrumentation and that there will be an alarm if the defined limit values are exceeded.

4.2.1.2 External Flooding

4.2.1.2 (1) The potential causes of external flooding shall be determined and considered site-specifically. For flooding hazards due to high water levels in the receiving water, a design basis flood shall be defined. Furthermore, heavy rainfall hazards at the plant site shall be considered.

4.2.1.2 (2) External flooding shall not inadmissibly impair the safety of the plant.

Regarding the design requirements for equipment of safety system to cope with a design basis flood level, the corresponding regulations of Section 2.4 of the "Safety Requirements for Nuclear Power Plants" shall apply.

4.2.1.2 (3) Permanent as well as temporary protection means shall be used for flood control, considering the regulations in subsection 4.1 (5).

4.2.1.2 (4) Apart from the static impact by water pressure, possible dynamic effects (e.g. wave actions or impact of flotsam) shall be considered.

4.2.1.3 Extreme meteorological conditions

4.2.1.3 (1) The following extreme meteorological conditions shall in particular be considered site-specifically:

- High or low ambient air or cooling water temperatures,
- Long-lasting droughts and their effects on cooling water supply,
- Storms including tornados,
- High or low humidity,
- Snowfall,
- Icing,
- Heavy rain, hail,
- Lightning stroke,

including accompanying effects such as salt deposits on electrical isolators, ingression of sand, or wind generated missiles.

4.2.1.3 (2) The possibility of a failure of supply systems (e.g. freezing of supply lines or operating materials) shall be considered.

4.2.1.3 (3) Suitable protection means shall ensure that extreme meteorological conditions will not inadmissibly impair the safety of the plant. It shall be specified in the operating procedures within which limits plant operation is admissible and how to proceed, if specified limit values are exceeded.

4.2.1.3 (4) Suitable protection means shall be in place, in particular against icing of items important to safety such as circulating water intake, inlet air supplies or the main-steam relief valves.

4.2.1.3 (5) Regarding the protection against impacts by storms, the following aspects shall be considered in particular:

- Wind speed,
- Gustiness,
- Suction effects,
- Total duration of the impact,
- Interaction with adjacent structures,
- Wind-related receiving water level.

4.2.1.3 (6) Regarding the protection against heavy rainfall, the following aspects shall be considered in particular:

- Flood level on the plant premises,
- Ingress of water into buildings,
- Missing possibilities of temporary measures,
- Ingress of water via drainage systems, and
- Impairment of the drainage systems.

4.2.1.3 (7) Lightning protection shall be in place to ensure that items important to safety are not inadmissibly impaired by the effects of lightning.

4.2.1.3 (8) In line with the plant requirements, lightning protection shall consist of measures for interception and grounding of lightning strikes and of plant internal measures for reduction and limitation of overvoltage.

4.2.1.3 (9) Lightning protection devices shall be as far as possible reviewed periodically.

4.2.1.4 Biological hazards

4.2.1.4 (1) The following biological hazards shall in particular be considered plant-specifically:

- Mussel growth,
- Larger quantities of algae, jellyfish or fish,
- Larger quantities of foliage or grass as flotsam,
- Larger quantities of biological flotsam due to flooding,
- Microbiological corrosion.

4.2.1.4 (2) Suitable protection means shall ensure that biological impacts do not inadmissibly impair the safety of the plant. In particular, the clogging of cooling and ventilation systems shall be prevented.

4.2.1.4 (3) Safety related cooling water and ventilation systems shall be easy to clean and maintain.

4.2.1.4 (4) The necessary cleaning equipment shall be in place on site.

4.2.1.4 (5) The receiving water shall be regularly monitored for any changes regarding the biological conditions.

4.2.2 Very rare human-induced external hazards

4.2.2.1 Aircraft crash

4.2.2.1 (1) Suitable protection means shall ensure that the safety of the plant is not inadmissibly impaired by an (accidental) aircraft crash.

4.2.2.1 (2) Vibrations induced by the impact of an aircraft shall be considered.

4.2.2.1 (3) The effects of debris/missiles, kerosene fires, kerosene explosions and other consequential effects shall be considered, in particular:

- Kerosene fires at the plant site,
- Kerosene explosions outside of buildings,
- Fire or explosion of (liquid or vaporous) kerosene having penetrated into buildings either through permanent openings or those caused by the crash,
- Intrusion of combustion products and intake air with reduced oxygen content due to combustion processes into ventilation systems potentially affecting operator actions, electrical installations and the diesel generator supply air systems.

Note:
The protective effects of structures in front of the one involved in the crash may be considered.

For redundant systems, protection against aircraft missiles may also be achieved by physical separation.

4.2.2.1 (4) Impacts (e.g. debris/missiles and fires) due to (accidental) aircraft crashes near the plant shall also be considered.

4.2.2.1 (5) The design shall be based on the following load assumptions:

- Impact-load time diagram:
- Impact time [ms / Impact load [MN]

Impact time [ms]	Impact load [MN]
0	0
10	55
30	55
40	110
50	110
70	0

- Impact area: 7 m^2 circular.
- Impact angle: normal to the tangential plane at the point of impact.

4.2.2.1 (6) Structures shall be designed to ensure full protection if equipment of the safety system or emergency equipment needed to control events from an aircraft crash are either located inside the building structure or behind it. The protection shall ensure that the components are not damaged by fragments and debris/missiles to such a degree that in case of their failure it can no longer be ensured that the plant can be brought into a safe state.

Permanently existing openings in building in which equipment of the safety system is located shall be arranged and protected such that in the event of an aircraft crash no kerosene can penetrate into these buildings.

If penetration of kerosene cannot be prevented by the arrangement and protection of permanent openings, these openings shall be arranged and protected at least such that the equipment of the safety system being necessary as specified is not inadmissibly impaired.

4.2.2.1 (7) The ion exchangers of the coolant purification system, associated spent-resin tanks and other systems and components containing comparably high amounts of activities being combustible in principle shall be protected against damage by dedicated structural and fire protection means in order to avoid any significant release of radioactive materials due to kerosene fires.

4.2.2.2 Plant external explosion

4.2.2.2 (1) Suitable protection means shall ensure that site-specifically postulated plant external explosions do not inadmissibly impair the safety of the plant. Apart from chemical explosions, explosions of vapour, gas or liquid clouds, deflagration-to-detonation transition (DDT) and physical explosions shall be considered.

4.2.2.2 (2) Local as well as large-scale explosion effects shall be considered.

4.2.2.2 (3) Suitable protection means against the effects of plant external explosions are in particular the design of structural elements and the adherence to safe distances.

4.2.2.2 (4) For the structural design, the following impacts shall be particularly considered:

- Direct, reflected and focussed pressure waves,
- Time dependent course of positive and negative pressure,
- Debris,
- Vibrations of soil and structures,
- Thermal impacts.

4.2.2.2 (5) For the structural design, the pressure variation in time according to the guideline for the protection of nuclear power plants against pressure blast waves from chemical explosions (BMI 1.8.1976 - RS I 4 - 513 145/1) shall be postulated, unless there are indications of higher pressure variations in time to be expected.

4.2.2.2 (6) Ventilation systems important to safety and necessary for the control of the explosion impacts shall not be inadmissibly impaired by the effects of an explosion.

4.2.2.3 Hazardous materials

4.2.2.3 (1) The following shall be understood as hazardous materials:

a) Materials that may lead to a short - or long-term failure of the required function of items important to safety. These are:
   - Explosive materials,
   - Flammable materials,
   - Materials displacing or consuming the oxygen in diesel supply air,
   - Clogging materials, or
   - Corrosive materials.

b) Materials endangering the shift personnel's required capability of action. These are:

- Toxic materials,
- Narcotic materials,
- Caustic materials,
- Materials displacing oxygen,
- Oxygen consuming materials, or
- Explosive materials and
- Radioactive materials.

4.2.2.3 (2) Suitable protection means shall ensure that hazardous materials do not inadmissibly impair the safety of the plant and the personnel's capability of action.

In this context, the following aspects are relevant:

- Site-specific occurrence of hazardous materials (stationary or on transport routes),
- Possibilities of their ingress into buildings or systems,
- Their impact mechanisms, including time history (e.g. of the concentration) as well as
- possible options for their detection and monitoring.

4.2.2.3 (3) For the detection of hazardous materials and for the initiation of necessary operator actions, corresponding organisational procedures and, to the extent required and possible, protection means shall be in place.

4.2.2.3 (4) Depending on nature and impact of the hazardous materials, the following protection means shall particularly be considered apart from the necessary systems design (e.g. physical separation of openings of redundant subsystems):

Plant specifically:

a) For hazardous materials with short-term impact:

- Interruption of the media supply (e.g. ventilation isolation),
- Change in the mode of operation (e.g. from supply air/exhaust air operation to recirculation mode),

b) For hazardous materials with long-term impact:

- Inspection of potentially impaired equipment and precautionary measures, including recurrent testing and inspections and
- Cleaning of the above mentioned equipment and measures.

c) Organisational:

- Training of the personnel,
- Protection of the personnel by e.g. provision of breathing apparatus, establishment of areas of independent media treatment (e.g. air conditioning/regeneration).

d) In addition:

- Detection devices for the respective hazardous materials in the supply openings, in the main control room, on the power plant premises and, where required, in the vicinity of plant components at risk, however with priority in the vicinity of the potential source of hazardous materials,
- Communication links to the locations where hazardous materials are handled,
- Prevention of long-term contact with corrosive materials,
- Protective coatings, and
- Safety distances.

4.2.2.3 (5) Accessibility and habitability of the main control room or the supplementary control room shall also be ensured to the extent required during the impact of hazardous materials by provision of protective equipment.

4.2.3 Other human-induced hazards

4.2.3.1 Flotsam, dam failures and ship accidents

4.2.3.1 (1) The essential service water supply required for safety reasons shall be also ensured according to site-specific requirements in case of

- Impacts by flotsam,
- Loss of cooling water due to failure of a downstream dam,
- Consequences from ship accidents, and
- Collisions of ships with cooling water intake structures.

4.2.3.1 (2) The effects of ship accidents on the essential service water supply, e.g. deterioration of the water quality due to contamination with oil or other hazardous materials shall be considered.

4.2.3.2 Plant external fire

4.2.3.2 (1) Suitable protection means shall ensure that plant external fires do not inadmissibly impair the safety of the plant.

4.2.3.2 (2) Apart from thermal impact, combustion products such as aerosols and toxic and/or corrosive materials shall also be considered.

4.2.3.2 (3) The effects of plant external fires on ventilation systems and the intake air of the emergency diesel generators as well as the potential ingress of combustion products into buildings shall be considered.

4.2.3.2 (4) Ground level ducts and openings of underground supply equipment or buildings shall be protected against intrusion of flammable liquids.

4.2.3.3 Electromagnetic impacts (except lightning)

4.2.3.3 (1) Sources of electromagnetic interferences outside the plant whose impacts on the safety system, the emergency equipment or further equipment necessary for safety cannot be prevented shall be comprehensively identified and their possible effects shall be assessed. The consideration of enveloping impacts is

permissible. An electromagnetic compatibility (EMC) analysis shall be performed to the extent required and shall be submitted for review.

4.2.3.3 (2) As far as electromagnetic interferences from outside the plant may impair the function of equipment referred to in subsection 4.2.3.3 (1), means shall be in place for protection of the respective I&C systems in accordance with their safety significance.

4.2.3.3 (3) During the entire plant operating lifetime, the protection of equipment referred to in subsection 4.2.3.3 (1) against electromagnetic interferences shall be adapted to changes of electromagnetic sources outside the plant.

4.2.3.3 (4) Electromagnetic compatibility in their operating environment shall be demonstrated by appropriate tests (EMC demonstration) for equipment referred to in subsection 4.2.3.3 (1) that may be impaired by electromagnetic impacts from outside the plant.

Annex 4 of the

„Safety Requirements for Nuclear Power Plants“:

Principles for applying the single failure criterion and the maintenance

22 November 2012

Structure

1 The single failure concept - Principles for applying the single failure criterion

Objective of the single failure criterion

1 (1) The single failure concept is a deterministic concept for the design of safety-relevant equipment listed in Sections 2.2 to 2.5. The postulation of a single failure and where required a maintenance case ensures sufficient redundancy for safety related equipment when demanded.

1 (2) The degree of redundancy of equipment required to ensure a safety function depends on its safety relevance within the defence-in-depth concept and to cope with event initiated by internal and external hazards. Section 2 contains the relevant regulations.

1 (3) If an equipment is designed according to the single failure concept, it can be assumed with sufficient certainty that its operability is not dependent on a coincidental failure of any particular component of the equipment or on the presence of a maintenance case. The related design shall comprise all components of the safety-relevant equipment and all necessary supply functions like instrumentation and control equipment, and other support functions.

1 (4) The objective of the postulation of a single failure in passive plant components is an appropriate segregation of redundant safety related equipment. Segregation shall be such that there will be no failure of safety-relevant equipment referred to in subsection 1 (1) as a consequence of a postulated passive single failure.

1 (5) In connection with the single failure concept, the allowable period of inoperability of safety-related equipment referred to in subsection 1 (1) as a consequence of maintenance activities is also of relevance as these have effects on the overall reliability of the safety function concerned. Thus, for ensuring the required reliability, the allowable period of inoperability due to maintenance is specified within the framework of the single failure concept dependent on the type of maintenance and its impact on plant safety. Section 3 specifies the relevant requirements.

2 Regulations for applying the single failure concept

2.1 General requirements

2.1 (1) If a single failure has to be postulated, it generally must be postulated for active as well as for passive equipment. Exceptions or system and component specific requirements are given in Section 2.5, further exceptions shall be justified.

2.1 (2) A single failure in redundant equipment of the safety system, emergency equipment or further equipment necessary for safety shall not induce safety-relevant loss of functions in other redundants of these equipment.

2.1 (3) Regarding the safety demonstration, the single failure leading to the worst effect with regard to the related acceptance criterion shall be postulated, as well as, as far as to be postulated, the combination of a single failure with a maintenance case leading to the overall worst effect. The choice shall be justified.

2.1 (4) If several safety-relevant equipment for a particular safety function, according to Sections 2.2.2, 2.2.3, 2.3 and 2.4, have to fulfil their tasks simultaneously or successively to cope with a postulated event, the occurrence of a single failure shall be postulated for the total of the equipment, but not simultaneously in more than one of them.

2.2 Redundancy requirements for safety-relevant equipment during operational modes A and B

2.2.1 Redundancy requirements for equipment of level of defence 1

For equipment of the level of defence 1, no redundant design is required (degree of redundancy n+0).

2.2.2 Redundancy requirements for equipment of level of defence 2

For equipment required to cope with events on level of defence 2, neither a single failure nor the unavailability of a redundant equipment due to maintenance (maintenance case) shall be postulated (degree of redundancy n+0). As an exception a single failure shall be postulated for instrumentation and control functions of Category B (degree of redundancy n+1).

Note:
If safety equipment is activated in case of events on level of defence 2, e.g. in case of „loss of main heat sink“ and „loss of offsite power $\leq$ 10 hours“, the single failure and the maintenance case are covered by the loss of failure postulates on level of defence 3.

2.2.3 Redundancy requirements for equipment of level of defence 3

For the safety equipment required to cope with events on level of defence 3, a single failure generally combined with a maintenance case shall be postulated when demanded (degree of redundancy n+2). For exceptions, see below.

If for a safety equipment, only a redundancy degree of n+1 is implemented (e.g. for primary circuit or containment isolation valves), maintenance is only allowed if during maintenance on such an equipment, its safety function can be reliably ensured by other measures (e.g. closure of the 2nd isolation valve), or the maintenance is sufficiently restricted in time und the permissible unavailability is specified in the operational documentation.

Regarding maintenance, all types of maintenance permitted and possible to be performed during an operational mode shall be considered. Details about the permissibility of maintenance during different operational modes are provided in Number 3.

Note:
A postulated ineffectiveness of the most reactivity effective control rod element may be treated as a single failure in the safety demonstration regarding the sub criticality acceptance criterion according to „Safety Requirements for Nuclear Power Plants“ subsections 3.2 (6) and (7).

If the first actuation of the reactor protection system is not credited in the safety demonstration, according to Annex 5 of the “Safety Requirements for Nuclear Power Plants” subsection 3.2.4 (2), a simultaneous single failure on active equipment shall be postulated, albeit only after a period of 100 hours in the case of simultaneous maintenance.

2.2.4 Redundancy requirements for equipment of level of defence 4a

In case of events on level of defence 4a, neither a simultaneous occurrence of a single failure nor a simultaneous maintenance case shall be postulated (degree of redundancy n+0). Details about the permissibility of maintenance during different operational modes are provided in Section 3.

2.2.5 Redundancy requirements for equipment of level of defence 4b and 4c

For equipment of level of defence 4b and 4c, neither a single failure nor a maintenance case are required (degree of redundancy n+0).

2.3 Redundancy requirements for safety-relevant equipment during operational modes phases C to F

2.3 (1) For the periods of planned maintenance during operational modes C to F outage, shut-down states) on equipment of level of defence 3 required for these operational modes, a single failure shall be postulated without an additional maintenance (degree of redundancy n+1).

2.3 (2) A degree of redundancy n+0 is permissible in the operational modes E and F if in case of a loss of function of the safety-relevant equipment, relevant acceptance criteria are not exceeded within 10 hours and the active safety-relevant equipment failed or being under maintenance can be made functional within this time frame.

2.4 Redundancy requirements for equipment required to cope with very rare human-induced external hazards

2.4 (1) For safety-relevant equipment required to cope with very rare human-induced external hazards in all operational modes neither a single failure nor a maintenance case have to be postulated (degree of redundancy n+0).

2.4 (2) For the function of equipment required to cope with very rare human-induced external hazards within the first 30 minutes after the impact, a single failure in active system components of these equipment shall be postulated (degree of redundancy n+1). For equipment not required within the first 30 minutes, neither a single failure nor a maintenance case shall be postulated (degree of redundancy n+0).

2.5 System and component specific requirements for the application of single failure criterion

Passive plant components

2.5 (1) In the single failure concept, a failure of passive equipment needs not be postulated if it is demonstrated that this equipment is designed in accordance with the following requirements:

- Consideration of maximum load/stress in all relevant conditions during operation and of all predictable changes in material property conditions with sufficient factors.
- Use of suitable materials for the intended functions and conditions.
- The equipment is manufactured, assembled, tested and operated based on a comprehensive quality assurance system to ensure the required reliability.

The measures and safety factors to be applied shall be defined also according to the safety significance of the safety equipment.

2.5 (2) The safety demonstration required in subsection 2.5 (1) can be considered as verified if the requirements regarding design, construction, material selection, manufacturing and testability of the equipment are fulfilled according to regulations taking the safety significance of the equipment into account.

Valves

2.5 (3) For check valves, a single failure has to be postulated if, they have to change their initial position to fulfil a required safety function.

2.5 (4) For self-medium-operated safety valves, relief valves and isolation valves of the reactor coolant system and the main steam system, in case of demand, the single failure shall to be postulated within the pilot assemblies, not in the main valve.

3 Maintenance

3.1 General requirements for maintenance

3.1 (1) Maintenance resulting in unavailability of safety-relevant equipment referred to in Sections 2.2 to 2.5 not compensated by special measures replacing their function or making their functionality unnecessary (e.g. reactor shutdown, power reduction, use of other systems), is permitted only, if the requirements of the single failure concept according to Section 2 are fulfilled during the maintenance. This principle shall also be applied to other measures resulting in an unavailability of safety-relevant equipment, e.g. in the case of plant hardware or operational modifications.

3.1 (2) For the restoration (repair) of the function of a failed safety-relevant equipment according to subsection 3.1 (1), allowable periods of inoperability shall be defined in the plant operational documentation. Details are provided in Section 3.2.2.

3.1 (3) Furthermore, conditions and requirements for preventive maintenance, especially for preventive maintenance in power operation, shall be defined in the operational documentation. Details are provided in Section 3.3.

3.2 Maintenance measures for restoration of the specified normal condition of safety-relevant equipment (repair)

3.2.1 Measures in case of identified deficiencies on safety-relevant equipment

3.2.1 (1) In case of identified deficiencies on safety-relevant equipment resulting in unavailability of the equipment, immediate actions to identify the cause of the deficiency and for the elimination of the deficiency shall be initiated. In particular it has to be clarified, whether the damage mechanism is of systematic nature.

3.2.1 (2) Plant operation measures (e.g. power reduction, plant shutdown), shall be initiated according to the plant operating procedures. These plant operating procedures shall be identified and defined according to Section 3.1.

3.2.1 (3) If a deficiency identified cannot be corrected within the allowable period of inoperability, the plant shall be brought into the operational mode required by the plant operating procedures.

3.2.1 (4) If it is predictable that in case of an identified deficiency on a safety-relevant equipment, the repair cannot be performed within the allowed period of inoperability, measures according to the requirements in Section 3.1 shall be initiated immediately.

3.2.1 (5) In cases where the plant operating procedures do not specify explicitly allowed periods of inoperability for a safety-relevant equipment, the plant shall immediately be brought into an operational mode in which the availability of this equipment is not required or is required only to a limited extent.

3.2.2 Specification of allowable periods of inoperability

3.2.2 (1) The allowed periods of inoperability of equipment required to cope with events on levels of defence 2 to 4a shall be determined in consideration of the reliability analyses, as far as necessary; and shall be identified in consideration of operating experience and specified in the plant operating procedures.

3.2.2 (2) These specifications shall include at least the following information:

- Allowed periods of inoperability of one or more of this equipments and their minimum availability required for each of the operational modes.
- Clear description of the measures to be initiated when reaching the allowed periods of inoperability (e.g. power reduction or manoeuvre into a required plant operational mode, further measures to reduce the probability of initiating events).

3.2.2 (3) For cases which are not specified in detail in the plant operation conditions, the plant operation conditions shall include guidance on how to identify an appropriate operational mode, an operational mode in which the availability of the affected equipment is not required or is only required to a limited extent.

3.3 Preventive maintenance on safety-relevant equipment

3.3.1 General requirements for the preventive maintenance

3.3.1 (1) Preventive maintenance beyond the scope of maintenance measures according to Section 3.3.2, and resulting in unavailability of safety-relevant equipment, according to subsection 3.1 (1), shall be performed in general during operational modes in which an actuation of this equipment is not necessary or is rather unlikely, as a rule during the operational modes C – F.

3.3.1 (2) During the operational modes A and B, preventive maintenance measures are only permissible to a limited extent and only in compliance with the requirements of Section 3.3.3.

3.3.1 (3) Requirements for the preventive maintenance of safety equipment shall correspondingly also apply to other planned measures leading to an unavailability of safety-relevant equipment (e.g. due to plant modifications). Deviations shall be justified.

3.3.2 Servicing

If servicing is required for ensuring the functional operability of safety-relevant equipment, it can be performed in all operational modes if the following conditions are met:

- The servicing requires only unavailability of the safety-relevant equipment less than 8 hours, and
- The safety-relevant equipment can be brought back to functionality in short time in case of a necessary demand, this shall also be possible under the conditions of an accident happened, and
- The servicing activities are limited to one redundant only and all other redundants remain fully available during this period, and
- During start-up and shutdown of the plant, servicing is limited to unavoidable cases.

3.3.3 Requirements for preventive maintenance in operational modes A and B (on power preventive maintenance, OPM)

3.3.3 (1) The duration and the boundary conditions under which preventive maintenance (OPM) on equipment required to cope with events on level of defence 2 to 4a, due to internal and external hazards, as well as due to very rare human-induced external hazards during operational modes A and B is permissible shall be specified in the plant operating procedures with consideration of the safety-related requirements.

3.3.3 (2) Regarding the specifications of subsection 3.3.3 (1), the following requirements shall be fulfilled:

- In case of n+3 and higher redundant safety-relevant equipment, there are no limitations for OPM in a single redundant. Criteria in accordance with subsection 3.3.3 (3) shall be met, irrespective of the degree of redundancy of the safety- relevant equipment.
- For n+2 equipment of level of defence 3, the time of unavailability due to OPM shall be restricted under consideration of the reliability requirements for the respective safety equipment. Without a detailed safety demonstration, for n+2 equipment, the duration of unavailability shall not exceed 7 days per redundant and year. For longer periods, plant-specific safety analysis shall be presented showing that unavailability of this safety equipment over a longer period does not

raise any safety concern. OPM on equipment of level of defence in depth 3 with a degree of redundancy less than n+2 are not permissible.

- Equipment of level of defence 2 with a required degree of redundancy of n+1 must not be subject to OPM unless sufficient reliability of the equipment was demonstrated through assessments considering the relevant safety relevant events.
- Equipment of level of defence 4a and emergency equipment must not be subject to OPM unless sufficient reliability of the equipment was demonstrated considering the relevant events.

3.3.3 (3) OPM measures are only permissible if the following boundary conditions are fulfilled:

- The OPM measure shall not lead to a noteworthy increase of probability for events on levels of defence 2 and 3.
- OPM measures shall not be performed in several redundants at the same time and shall be limited to one redundant. Furthermore it shall be ensured that the availability of the remaining redundants is not limited due to other activities, e.g. modification measures. This does not apply to necessary repair activities on safety-relevant equipment if those had failed coincidentally.
- The OPM measure shall not lead to loss of functions, especially not due to common-cause failures, of safety-relevant equipment not being affected.
- The fulfilment of maintenance requirements in case of OPM shall also be ensured under the conditions of operational modes A and B (e.g. requested post maintenance testing not affected).
- During start-up and shutdown of the plant and related test periods, no OPM shall be performed.
- The integrity of the barriers reactor coolant pressure boundary and containment, as well as the reliability of their active safety-related functions shall not be impaired by OPM measures in an undue manner. As far as only two isolations (n+1) are available as barriers, OPM measures on these isolation devices are acceptable if the cooling circuit is depressurized.

4 Ensuring functionality of safety-relevant equipment

4 (1) The function of safety-relevant equipment shall be subject to in-service inspections in the required scope under conditions that correspond to the real situation as far as possible.

4 (2) If possible, the entire functional sequence of the equipment shall be subjected to functional tests similar to the functional sequences during the event; including al- so connecting the emergency power supply to the consumers. If only partial test sequences are possible for process-related reasons, sufficient overlapping of the various partial test sequences shall be ensured.

4 (3) Function tests shall not lead to a noteworthy increase of the probability for events on levels of defence 2 and 3.

4 (4) The functionality of the equipment shall also be maintained during the functional test as far as possible. Where applicable, unavailability time intervals due to functional tests shall be considered in the reliability analysis.

4 (5) If a safety-relevant piece of equipment has to be positioned in a dedicated stand-by position during operation and this position has to be changed in the course of a functional test, it shall be ensured that the equipment can be brought back into the requested position in due time in case of safety-relevant demands.

4 (6) To ensure the functionality of a safety-relevant equipment, all planned or unplanned individual component unavailability, resulting in a unavailability of the equipment, shall be easily identifiable for the operating personnel (e.g. deviation from required stand by position, unavailability due to maintenance, loss of function of instrumentation and control equipment, unplanned changes of fill levels).

4 (7) False positioning of valves shall be prevented by reliable technical equipment (e.g. fault alarm in case of deviation from required stand-by position, valve locks), if necessary in connection with reliable administrative measures.

4 (8) Deviations from parameter values specified in the plant operating procedures for ensuring safe plant operation shall be indicated to the operating personnel by o tic and acoustic signals in the main control room.

4 (9) It shall be ensured that in case of an event, all information necessary for the verification of functionality and effectiveness of required equipment shall be available for the operating personnel in the main control room or in the supplementary control room or the information can be easily and rapidly determined by using the information available in the main control room or in the supplementary control room.

4 (10) After the completion of maintenance activities on safety-related equipment, the functionality and the verification of required functions shall be ensured by qualified post maintenance functional tests.

Annex 5 of the

"Safety Requirements for Nuclear Power Plants":

Requirements for Safety Demonstration and Documentation

22 November 2012

Structure

1 Objective

1 (1) This regulation contains requirements for safety demonstrations and documentations. Suitable demonstration methods shall be applied to verify fulfilment of the requirements specified in the "Safety Requirements for Nuclear Power Plants".

Note:
In the following, general requirements are formulated for safety demonstration and documentation.
Detailed requirements for the safety demonstration of loss-of-coolant accidents can be found in Appendix 1. Detailed requirements for the determination of differential pressures within the containment can be found in Appendix 2. Detailed requirements for the determination of jet and reaction forces in the case of leaks in pressurised systems within the containment can be found in Appendix 3. Further technical requirements may be found in dedicated technical regulations.

1 (2) According to subsection 5 (2) of the "Safety Requirements for Nuclear Power Plants", deterministic and probabilistic methods shall be applied for safety demonstrations:
The deterministic methods comprise

a) the computational analysis of events and states,

b) the measurement or experiment,

c) the engineering assessment.

The deterministic methods form the basis for the performance of system assessments. In addition to the results gained from applying deterministic methods, results from probabilistic analyses are included to the required extent in the system assessment. The system assessment serves the demonstration that the requirements for the effectiveness and reliability of the measures and equipment on the different levels of defence are fulfilled.

1 (3) The safety demonstrations shall be documented in the form of complete and comprehensible documents.

2 Fundamental requirements for the system assessment

2 (1) The system assessment shall show that the required effectiveness and reliability of measures and equipment as well as their essential quality characteristics are fulfilled. It shall take into account the states that result from the computational analysis of selected events or conditions.

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 as well as the condition of the safety-relevant measures and equipment concerned. Where applicable, planned modifications shall be taken into account, including information about the tasks to be done 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) If relevant to the assessment of safety, the results of the evaluation of operating experience shall be included in the system assessment.

3 Fundamental requirements for the deterministic analysis of events or states

3 (1) The analysis of events or states shall demonstrate that the quantitative acceptance criteria specified in the "Safety Requirements for Nuclear Power Plants" are fulfilled.

3 (2) If safety demonstration is done by analysing events or states,

a) up-to-date compilation of safety-relevant information on the prevailing condition of the safety-related measures and equipment concerned shall be used, and where applicable, taking into account planned modifications;

b) validated analysis methods according to the requirements in Section 3.1 shall be used for the respective areas of application;

c) selected initial and boundary conditions shall be used in the analyses based on the requirements listed in Section 3.2;

d) the uncertainties that are associated with the respective analytical results for the corresponding acceptance criterion in connection with levels of defence 1 to 3 shall be 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 analytical results in connection with level of defence 4 shall be assessed with regard to the acceptance target.

3 (3) If safety demonstration is done by analysing events or states, the following shall be documented in particular:

a) the relevant data used; unless plant-specific data are used, their applicability shall be justified;

b) the justification of the choice of the underlying impacts, events, operational modes and operating conditions with regard to the fulfilment of the respective acceptance criterion;

c) when using statistical methods, the determination of the uncertainty of the analytical result, 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 must be validated for their respective scope of application.

3.1.1 (2) If calculation methods are used for analysing the effectiveness of preventive or mitigative accident management measures, these shall be validated for their respective scope of application.

3.1.1 (3) The validation of an analysis method must comprise the examination of the scope of application of the method as well as the examination of the agreement of the results that can be obtained by application of this method with comparative values obtained from

a) experiments, test data, plant operation, plant transients or other events,

b) analytical solutions, or

c) other validated analysis methods.

3.1.1 (4) An analysis method may be deemed validated if 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. This is especially true if the results obtained with the method lie within the band- widths of experimentally obtained results (see subsection 3.1.2 (2)).

3.1.2 Implementation

3.1.2 (1) The validation shall be 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 shall cover in 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 shall be demonstrated.

3.1.3 Documentation

3.1.3 (1) The documentation regarding validation must include:

a) data relating to the comparative values used (according to subsection 3.1.1 (3)), for experiments, test data, plant operation, plant transients or other events, including data on the accuracy of the comparative values referred to,

b) data on the validated scope of application of the analysis method,

c) 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 Requirements regarding 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 relevant mechanical, chemical and thermal impacts shall be considered.

a) The impacts that may result due to the conditions, events and defined operating conditions on levels of defence 1 to 3 as well as due to internal and external impacts have to be postulated or assumed to occur simultaneously such that all effects are considered conservatively.

b) Concerning impacts resulting from very rare human-induced external hazards, 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 may be assumed realistically.

3.2.1 (2) For the demonstration of the integrity and support stability of components, the relevant mechanical, chemical, thermal and radiation-induced impacts shall be considered.

a) The impacts that may result due to the conditions, events and defined operating conditions on levels of defence 1 to 4a as well as due to internal and external impacts have to be 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.

b) Concerning impacts resulting from very rare human-induced external hazards, the permissible loading of the 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 taken into account realistically. In the weakest locations, the integrity of the load-carrying cross-sectional areas has to 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 may be assumed realistically, and the effects on the condition of the components may be ana- lysed correspondingly.

3.2.1 (3) Combinations of several external impacts or combinations of these impacts with internal events shall be postulated according to subsection 4.2 (1) of the "Safety requirements for Nuclear Power Plants".

The accidental impacts and the impacts resulting from the accident consequences shall be combined with the "normal external operational loads" (including 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.

3.2.1 (4) As event-induced consequential events due to external impacts as well as very rare human-induced external hazards the possibility for

a) impacts from burst pressure blast waves upon the failure of vessels, pipes and other containers with high energy content;

b) consequential mechanical damage upon the failure of plant components (including damage due to flying and falling fractured parts as well as jet and reaction forces);

c) plant-internal flooding due to the failure of plant components;

d) plant-internal fires and explosions;

e) increased radiation levels;

f) chemical reactions as well as

g) mailfunctions of electrical, instrumentation and control or process engineering equipment shall be take into account and

h) loss of off-site power

shall be postulated, unless the respective components are designed to withstand these impacts.

3.2.1 (5) The protection of buildings and components under very rare human-induced external hazards shall be verified on the basis of specified load assumptions. Here, induced structural and component vibrations shall also be considered.

3.2.1 (6) Safety demonstration on levels of defence 2 to 4a must extend from the occurrence of an event at least to reaching a controlled plant state, in which the plant may remain permanently.

The analyses relating to the effectiveness of the measures provided on levels of defence 4b and 4c should be carried out up to the point where the state of the plant that is relevant for the analysis is reached.

3.2.1 (7) When quantifying the uncertainties of results according to Section 3.3, measurement and calibration errors may be considered statistically. If safety demonstration is done conservatively bounding according to Section 3.4, the measurement and calibration errors shall be bounded by the values for initial and boundary conditions.

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 to be considered, taking into account the possible changes and oscillations during normal operation.

3.2.3 Level of defence 2 (abnormal operation)

3.2.3 (1) Adverse initial conditions lying within the range of realistic operating conditions shall be postulated for the different operational modes with regard to the respective acceptance criteria.

3.2.3 (2) All measures and equipment 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) An event independent loss of off-site power needs not be assumed.

3.2.4 Level of defence 3 (accident)

3.2.4 (1) The initial plant conditions to be assumed

a) for a safety demonstration according to Section 3.4 shall bound the worst case for the different operational modes with regard to the respective acceptance criterion, or

b) for safety demonstrations according to Section 3.3 shall be realistic parameter values, taking into account their uncertainty range.

3.2.4 (2) For demonstration of the effectiveness of measures and equipment on level of defence 3, the single-failure concept according to subsection 3.1 (7) of the "Safety Requirements for Nuclear Power Plants" as well as according to Annex 4 of the "Safety Requirements for Nuclear Power Plants" shall be applied.

In the analysis of events of level of defence 3, failure of the first actuation of the reactor protection system or the first actuation of reactor scram shall be postulated, unless only one actuation criterion is available due to physical and technical reasons.

In case of a postulated failure of the first actuation, the simultaneous occurrence of a single failure in active equipment shall be assumed, albeit only after a period of 100 hours in the case of simultaneous maintenance.

The postulated failures according to the subsections 3.2 (6) and 3.2 (7) of the "Safety Requirements for Nuclear Power Plants" shall be taken into account.

3.2.4 (3) A loss of station service power supply occurring simultaneously or - depending on the event - with a time lag shall be postulated for all measures and equipment necessary for accident control if this will have an adverse effect on the event sequence. Emergency power supply shall be considered in the analysis according to the switch-on programme of the devices supplied with emergency power.

3.2.4 (4) In case of loss-of-coolant accidents, when determining the effects of

a) the pressure and temperature build-up in the containment,

b) the pressure differences in the containment,

c) missiles, jet and reaction forces, and

d) pressure blast waves within the reactor coolant pressure boundary as well as

e) when demonstrating the effectiveness of the emergency core cooling system and the support stability of internals (especially large components) and rooms

the worst leak or break location for the different safety demonstrations, respectively, shall be determined and postulated for the range of leak and break sizes to be considered.

Note:
On this issue, see the enclosed Appendices 2 and 3, as well as Appendix 2 to Annex 2 of the "Safety Requirements for Nuclear Power Plants".

3.2.4 (5) In addition to the assumed loss of functions of the single-failure concept, safety demonstration shall also take into account accident-induced consequential loss of functions of measures and equipment with an adverse effect on the accident with regard to the acceptance target.

If relevant adverse influences on the event sequence may result in case that measures and equipment on levels of defence 1 and 2 will become operative during the event as specified, these influences shall be taken into account.

3.2.4 (6) The source term for radiological safety demonstrations on level of defence 3 shall be determined up until the end of the release. If necessary, suitable termination criteria shall be specified for defining the end of the release.

Note:
Detailed requirements for safety demonstration in connection with loss-of-coolant accidents are compiled in Appendix 1.

3.2.5 Level of defence 4a (anticipated transients without scram)

3.2.5 (1) In the analysis of anticipated transients without scram

a) realistic initial and boundary conditions can be chosen; the initial condition of the reactor core, however, shall assume the power operation at the most unfavourable point in time of the cycle (with xenon equilibrium) loading- and event-specific; additionally, with regard to reactivity feedback effects, values shall be applied that cover existing uncertainties;

b) all measures and equipment that have not failed due to the postulated event may be assumed to be available; if within the short-term range (until maximum pressure is reached) credit is taken of the switch-off of the main coolant pumps (PWR), the switch-off must be activated by instrumentation and control functions of Category A or B;

c) those changes in operating parameters and conditions that are caused by instrumentation and control processes shall be taken into account.

3.2.6 Level of defence 4b (events involving the multiple failure of safety equipment) and level of defence 4c (accidents involving severe damage on fuel assemblies)

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.

Note:
Sections 3.3 and 3.4 need not be applied for safety demonstrations for levels of defence 4b and 4c.

3.3 Quantification of the uncertainties of results

3.3 (1) When using statistical methods, the overall uncertainty of the respective analysis result shall be quantified according to subsection 3 (2) d). To this end

a) the parameters (initial and boundary conditions as well as model parameters) and models that have considerable influence on the uncertainties of the results shall be identified;

b) the ranges of uncertainty of the parameters identified that exist according to current knowledge shall be quantified, together with the parameter distributions if statistical methods are applied and,

c) where applicable, dependencies or interactions between individual input parameters shall be established and taken into account.

3.3 (2) Uncertainties of individual models not covered by a variation of parameters in the computer code shall be covered by biases added to the result which should be derived from the validation of the analysis method.

3.3 (3) If statistical methods are applied for the determination of the overall uncertainty, the one-sided tolerance limit in the direction of the acceptance criterion shall be determined, with a probability of at least 95% with a statistical confidence level of at least 95% to demonstrate the fulfilment of the acceptance criterion.

3.3 (4) Compliance with statistical acceptance criteria shall be 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 added to the analysis result, or

c) if with regard to the respective acceptance criterion

- most unfavourable parameter combinations are used that lie within the range of realistic operating conditions, or
- unfavourable values of the uncertainty range of the individual parameters are combined in a manner that the analysis result is not exceeded with a probability of at least 95%, or

d) if calculation methods or 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 requirements for safety demonstration by measurements

4 (1) Prior to the performance of measurements or experiments, the demonstration subject shall be specified and the measurement or experimental procedure shall be 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 shall be checked and set forth in writing. Relevant effects adverse to safety shall be avoided.

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 shall be justified. Any uncertainties in connection with the application of the results shall be identified.

4 (3) Safety demonstration by measurements and experiments shall take measurement uncertainties into account.

4 (4) The demonstration subject, the measurement or experimental procedure and the results shall be documented in a comprehensible manner.

5 Fundamental requirements 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 must rest 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 requirements for the performance of engineering assessments:

a) boundary conditions applied for the assessment, such as results and data from earlier calculations and tests shall be justified and documented,

b) the results of the assessment shall be documented completely and in a comprehensible manner,

c) if applied to interdisciplinary and complex issues, the engineering assessment shall be performed by an appropriately composed team.

5 (3) For ergonomic analyses of personnel actions, the tasks assigned to the personnel must be 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 requirements.

The task analysis must take into account the following aspects:

a) required and available information for the person acting,

b) required processes of information processing,

c) required decisions and individual actions,

d) time-dependent and spatial boundary conditions of the tasks.

6 Fundamental requirements for probabilistic safety analyses

6 (1) The fundamental methods and boundary conditions for the preparation of probabilistic safety analyses (PSAs) and the documentation requirements are described in the "Guide Probabilistic Safety Analysis".

6 (2) In PSAs for assessments according to subsections 5 (5a) and 5 (5b) of the "Safety Requirements for Nuclear Power Plants", up-to-date methods, models and data shall be used. The up-to-dateness of the PSA must consider in particular the following aspects:

a) safety-relevant modifications to measures, equipment or the operating mode performed in the plant,

b) safety-relevant events or phenomena that have become known and which are applicable to the German nuclear power plants mentioned in the scope of application of the "Safety requirements for NPP", and

c) the plant-specific evaluation of operating experience with regard to reliability parameters of components or occurrence frequencies of initiating events.

6 (3) In PSAs, plant-specific data shall be used. If no sufficient plant-specific data base from operating experience is available, generic data may be used. The applicability of the generic data shall be justified.

6 (4) PSAs shall be performed by qualified personnel of the licensee. Support by external personnel is permissible.

6 (5) The respectively required scope and level of detail of a PSA shall be specified with regard to the particular case.

7 Fundamental documentation requirements

7 (1) All documents that were or are used during the planning, construction and operation of the plant for the licensing and supervising procedure shall be documented in a systematic and comprehensible manner. The degree of detail of the documentation must be adapted to the safety-related significance of the contents of the documents.

7 (2) The documentation must meet the following requirements:

a) application of a clearance/licensing procedure that is commensurate with the relevance of the respective document,

b) clear identification of documents,

c) timely updating of documents, in particular in case of plant modifications,

d) identification of modifications and of the revision status of documents,

e) assurance of the availability of applicable documents at the respective locations of operation,

f) timely adaptation of documentation required for operation management to the current plant condition and keeping it available in the area of the main control room,

g) assurance of readability and visual clarity,

h) clear and unambiguous specification of safety-relevant operative instructions,

i) identification and distribution of external documents to the respective locations of operation,

j) prevention of the use of outdated documents or documents that are no longer valid.

7 (3) The documentation shall be maintained and archived according to defined rules. Rules for the maintenance and archiving of other documentation shall also be established.

7 (4) Fixings for the different kinds of document, documentation, document management, archiving, responsibilities and control shall be specified in a documentation system.

Appendix 1: Detailed requirements for the safety demonstration of loss-of-coolant accidents

A1 (1) To show the effectiveness of the emergency core cooling systems, analytical calculation demonstrations that are backed up by experiments shall be provided. Either the uncertainties of the analysis results shall be quantified according to Section 3.3 or a conservative safety demonstration shall be done according to Section 3.4, with the following underlying assumptions:

1. For both methods, the worst combination of the following shall be postulated:

   a) loss of function due to a single failure, b) unavailability due to a maintenance,

   b) loss of off-site power,

   c) initial power in the core (upon the onset of the accident, the most unfavourable values shall be assumed that can occur during specified normal operation with consideration of the variables regarding integral power, rod power, and power density distribution limited by the limitation of process variables equipment),

   d) point in time of the cycle, f) break location, and

   e) break size and break type.

Note:
Postulated leak cross-sections and breaks as well as further requirements for the boundary conditions of safety demonstration are contained in Annex 2, Appendix 2 as well as in Annex 5 of the "Safety Requirements for Nuclear Power Plants".

2. For the quantification of the uncertainties of results according to Section 3.3, measurement 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 measurement and calibration error regarding initial core power shall be 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 plant components shall be considered, unless corresponding provisions have been taken.

5. The mass flow resulting from the one-dimensional depressurisation calculation shall be reduced by 20% for the hot rod temperature calculation, with consideration of thermal-hydraulically induced flow distributions and possible cooling channel constrictions, as long as no dynamic calculations of cladding ballooning are performed.

6. To determine the suction head of the residual-heat removal pumps, calculations shall be 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 shall be 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,

   d) splash water and water accumulations that reach the reactor building sump only with delay or not at all.

8. The following shall be taken into account in the demonstration that core cooling is ensured for both the short and the long term:

   a) 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 equipment necessary for controlling the event; in determining the amount of the released material, the maximum leak size of 0.1 A may be assumed with regard to the main coolant pipe as far as the requirements for the break preclusion for the main coolant pipe are met, and

   b) the influence of released insulation and other materials that are carried into the core.

      The demonstrations shall be based on thermal-hydraulic boundary conditions which cover leak sizes including the double-ended rupture of the main coolant pipe.

9. For the analysis of the sufficient achievement and long-term retention of subcriticality, it shall be postulated for PWR that the secondary-side content of a steam generator mixes with the primary coolant and the coolant injected by emergency core cooling.

A1 (2) When demonstrating 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, the following shall be considered:

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 shall be calculated for at least 100 days after the onset of the accident. Here, it shall be assumed 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 shall be assumed that it will be released continuously with or from the coolant. The location of release shall be 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 shall be 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) As source of the radiolytically acting radiation, at least the equilibrium core at the end of the cycle that corresponds to the intended burn-up strategy shall be assumed. In doing so, the fission material and fission product composition of the fuel assemblies in the core and of the activation products shall be considered.

   b) The share of γ-decay heat absorbed in the coolant shall be 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 shall be shown that these assumptions lead to conservative results. Otherwise a time constant of 10% shall be 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 heat in the sump, values shall be applied for 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 shall be 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:

   a) 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),

   b) 0.5% of the spontaneous solids (99% deposition in the sump of the 0.01% released other solids and 0.5% other solids by leaching).

   It shall be assumed that 100% of their γ and β radiation energy is 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 shall be taken from the results of the emergency core cooling calculations.

7. Other metal-water reactions may not be considered if it can be shown that they release no important quantities of hydrogen.

Appendix 2: Detailed requirements for the determination of differential pressures within the containment

A2 (1) The determination of the differential pressures within the containment shall be based on the following requirements:

1. The initial condition assumed is the operating condition at 100% of the specified power.

2. According to subsections 2.1 (7) and 3 (9) of Appendix 2 ("Postulated leak cross-sections and breaks in the reactor coolant pressure boundary and in the external systems") to Annex 2 of the "Safety Requirements for Nuclear Power Plants", leak cross sections up to 2 A shall be postulated for the reactor coolant pipes.

3. If lumped-parameter models are used, a sufficiently fine nodalisation shall be chosen (at least one zone for each room considered).

4. Regarding the release of the energy and mass contents from the reactor coolant pressure boundary and defined adjacent systems, the maximum possible release rates at the start of the outflow process shall be postulated.

5. For each room the least favourable break situation shall be considered.

6. Heat transfer to the structures shall be determined conservatively. If experimentally evidenced heat transfer relationships are applied, the lower values of the existing range of uncertainties shall be considered.

7. The flow resistances occurring during the course of the overflow processes between the different rooms shall be considered realistically but assumed conservatively for the room in which the break is located. The assumptions made shall be 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 shall be specified conservatively for the differential pressure behaviour.

9. Assumptions that are not evidenced by experiments shall be made conservatively.

10. The added safety factor of the thus calculated maximum occurring differential pressures must be at least 15%. A value of at least 10,000 Pa shall be postulated for the differential pressure.

Appendix 3: Detailed requirements for the determination of jet and reaction forces in case of leaks in pressurised systems within the containment

A3 (1) When determining the effects caused by jet and reaction forces as well as by missiles on pressurised systems within the containment, the calculation shall be based on the following requirements:

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 Appendix 2 ("Postulated leak cross-sections and breaks in the reactor coolant pressure boundary and in the external systems") to Annex 2 of the "Safety Requirements for Nuclear Power Plants" apply. For these leaks, a stationary outflow shall be assumed for various break locations.

3. Free jet propagation and reaction on structures being in its way shall be considered.

4. The respective worst break location shall be chosen.

5. To calculate the reaction forces of the pipes, corresponding calculation models or experimentally evidenced relations shall be applied.

6. An added safety factor of 15% shall be applied with regard to the loading of the relevant safety-related plant components by jet forces and by the structural parts getting carried away and accelerated by these jet forces.